OSCE Organization for Security and Co-operation in Europe
Presence in Albania

Sapienza Università di Roma
Centro di Ricerca e Cooperazione con l'Eurasia, il Mediterraneo e l'Africa Sub-sahariana

INTERNATIONAL ACADEMIC CONFERENCE

THE ROLE OF TECHNOLOGY IN PREVENTING AND COMBATING ORGANIZED CRIME, FINANCIAL CRIMES AND CORRUPTION

Tirana, 21 June 2022

British Embassy Tirana

INTERNATIONAL ACADEMIC CONFERENCE

THE ROLE OF TECHNOLOGY IN PREVENTING AND COMBATING ORGANIZED CRIME, FINANCIAL CRIMES AND CORRUPTION

- BOOK OF PROCEEDINGS -

Tirana, 21 June 2022

Organization for Security and Co-operation in Europe
Presence in Albania

This publication was supported by the OSCE Presence in Albania in the framework of the project "Establishment of a Master's Programme in Criminology", financially supported by the Bureau for International Narcotics and Law Enforcement Affairs of the United States Government. The views expressed in this publication are those of the authors and do not necessarily reflect those of the OSCE Presence in Albania.

ISBN: 9789928470737

Design & printed by: Graphic Line-01
info@graphicline01.com

Board of the International Academic Conference

A. Project Manager

Dr. Alba Jorganxhi
National Legal Officer / Project Manager, OSCE Presence in Albania

B. Scientific Academic Board

Prof. Dr. Artan Hoxha
Rector, University of Tirana

Prof.Asoc.Dr. Dorina Hoxha
Dean, Faculty of Law, University of Tirana

Prof. Dr. Skënder Kaçupi
Lecturer, Faculty of Law, University of Tirana

Prof. Altin Shegani Ph.D.
Lecturer, Faculty of Law, University of Tirana

Prof.Dr. Eralda (Methasani) Çani
Lecturer, Faculty of Law, University of Tirana

Prof. Asoc. Dr.Ervin Karamuço
Lecturer, Faculty of Law, University of Tirana

Prof. Asoc. Dr. Lirime Çukaj
Head of Criminal Law Department, Faculty of Law, University of Tirana

Prof. Asoc. Dr. Engjell Likmeta
Lecturer, Faculty of Law, University of Tirana

Prof. Asoc. Dr. Skerdian Kurti
Lecturer, Faculty of Law, University of Tirana

C. Organizational Board

Prof Asoc. Dr. Enkeleda Olldashi
Lecturer, Faculty of Law, University of Tirana

Prof. Asoc. Dr. Kreshnik Myftari
Lecturer, Faculty of Law, University of Tirana

Dr. Adela Buçpapaj
Lecturer, Faculty of Law, University of Tirana

Dr. Ela Kerka
Lecturer, Faculty of Law, University of Tirana
Dr. Ivas Konini
Lecturer, Faculty of Law, University of Tirana

Table of Contents

Panel A - Technological Developments and Criminal Law
Moderator: Prof. Asoc. Dr. Ervin Karamuço

CORPORATE CRIMINAL LIABILITY AND NEW TECHNOLOGIES: DIGITAL COMPLIANCE STRATEGIES IN THEFIGHT AGAINST ECONOMIC CRIMES
Ph.D. Emanuele Birritteri **11-24**

PËRDORIMI I TEKNOLOGJISË, VIKTIMAT E KRIMIT DHE TË DREJTAT E SAJ NË SISTEMIN E DREJTËSISË PENALE NË SHQIPËRI
Prof. Dr. Vasilika Hysi **25-44**

DILEMA KUSHTETUESE MBI DËNIMIN PENAL NË BASHKËPUNIMIN E POSAÇËM
Magistrate Florian Kalaja **45 - 110**

CRIPTOVALUTE E CYBERCRIME. UN CONNUBIO DA NON SOTTOVALUTARE
Ph.D.c. Mattia Romano **111 - 118**

MBROJTJA JURIDIKO PENALE NDAJ MASHTRIMEVE TË LIDHURA ME KOMPJUTERAT
Ph.D. Ylli Pjetërnikaj & Ph.D. Adnan Xholi **119-142**

INTERNATIONAL CORRUPTION: CHARACTERISTICS AND IMPORTANCE OF THE INTERSTATUAL DISCIPLINE
Prof.Ersi Bozheku **143 - 146**

ORGANIZED CRIME AND THE USE OF TECHNOLOGY FOR COMMUNICATION PURPOSES
Magistrate Renis Sheshi & Ph.D. c. Alban Nako **147 - 160**

TECHNOLOGY, CYBERCRIME AND THE CRIMINAL LAWYER TRINITY. CHALLENGES IN ALBANIA
Ph.D. Jonad Bara & Ph.D. Brunilda Bara **161 - 173**

TEKNOLOGJIA DHE NDIKIMI I SAJ NË KRIMIN E ORGANIZUAR
M.Sc. Arfjona Duka & Ph.D. Iv Rokaj LLM **175 - 186**

VOTIMI ELEKTRONIK MES DETYRIMIT PËR TË SIGURUAR VOTIMIN E SHTETASVE JASHTË SHQIPËRISË DHE RREZIKUT PËR MASHTRIME ZGJEDHORE.
Ph.D. Vera Shtjefni & Ph.D. Lulzim Lelçaj **187 - 205**

KRIMI KIBERNETIK DHE SIGURIA KIBERNETIKE
M.Sc. Emiljano Likaj **207 - 239**

CYBERSTALKING - THE NECESSITY OF ADOPTING AN AD HOC CRIMINAL PROVISION, TO ENSURE AN EFFECTIVE PROTECTION OF VICTIMS IN THE DIGITAL AGE
M.Sc. Rojmir Hamzaj & M.Sc. Fjorisa Sharku **241 - 272**

E DREJTA E PRONËSISË INTELEKTUALE DHE MBROJTJA LIGJORE
Ph.D. Saimir Shatku & Ph.D. Mimoza Sadushaj **273 - 280**

KRIPTOMONEDHAT DHE PËRDORIMI I TYRE NË BOTËN KRIMINALE
M.Sc. Ina Veleshnja & M.Sc. Inva Koçiaj **281 - 293**

FACIAL RECOGNITION TECHNOLOGY (FRT): PROS AND CONS OF USAGE IN LAW ENFORCEMENT AGENCIES
M.Sc. Klea Xhaferri **295 - 309**

E DREJTA E PRONËSISË INTELEKTUALE DHE INTERNETI. MBROJTJA NGA LEGJISLACIONI PENALE NË SHQIPËRI.
Ph.D. Idlir Duhanxhi & M.Sc. Mariglen Tanushi **311 - 327**

MBROJTJA E JETËS PRIVATE SI PASOJË E VEPRAVE PENALE TË SHKAKTUARA NGA ZHVILLIMET TEKNOLOGJIKE
M.Sc. Eljona Ruçi **329 - 349**

ALTERNATIVAT E KRIMIT TË ORGANIZUAR NË SHQIPËRI DHE NDIKIMI I KRIMIT KIBERNETIK
Ph.D. Genada Taho **351 - 363**

Panel B - Scientific Methodology in Investigation and Criminal Litigation

Moderator: Prof. Asoc. Dr. Skerdian Kurti

TË HETOSH KORRUPSIONIN DHE KRIMIN EKONOMIK NËPËRMJET SIMULIMIT TË NJË AKTI KORRUPTIV. KUSHTET, KËRKESAT LIGJORE DHE STANDARDET E GJEDNJ-SË.
Magistrate Eliora Elezi Ph.D. & Magistrate Suela Xhani **365 - 380**

PËRDORIMI DHE ZHVILLIMI I TEKNOLOGJISË NË PARANDALIMIN DHE IDENTIFIKIMIN E VEPRAVE PENALE NË FUSHËN E PROKURIMIT PUBLIK.
Ph.D. Fjorida Ballauri & M.Sc. Josi Ballauri **381 - 394**

HIGH-TECH CRIMES AND CHALLENGES FOR THEIR INVESTIGATIONS
M.Sc. Ingrida Behri Mustafa **395 - 411**

NOW I SEE YOU: HOW TO BYPASS THE E2EE CONUNDRUM AND IDENTIFY PERSONS IN ACYBERCRIME ENVIRONMENT?
Ilvana Dedja LLM **413 - 428**

THE LIE DETECTOR THAT LIES? POLYGRAPH TEST IN THE EMPLOYMENT RELATIONSHIP OF PUBLIC SECURITY EMPLOYEES
M.Sc. Artemida Hoxhaj **429 - 447**

THE ROLE OF TECHNOLOGY IN CRIMINAL PROCEEDINGS AND ITS IMPACT ON THE RIGHT TOPRIVACY. ANALYSIS OF JUDICIAL PRACTICE OF AMERICAN SUPREME COURT AND EUROPEAN COURT OF HUMAN RIGHTS
M.Sc. Kiara Muka & M.Sc. Klea Cahani **449 - 467**

HYRJA NDËRKUFITARE NË SISTEMET KOMPJUTERIKE DHE PARIMI I SOVRANITETIT SHTETËROR
M.Sc. Ditmir Hoda **469 - 485**

ROLI I TEKNOLOGJISË NË PARANDALIMIN DHE LUFTIMIN E KRIMIT TË ORGANIZUAR, KRIMEVE FINANCIARE DHE KORRUPSIONIT
M.Sc. Ana Rushiti **487 - 498**

ALBANIAN CRIMINAL CODE AND PROTECTION OF VICTIMS OF TECHNOLOGY BY VIRTUAL CHALLENGES
Prof.Asoc. Ervin Karamuço **499 - 507**

PASTRIMI I PRODUKTEVE TË VEPRËS PENALE OSE VEPRIMTARISË KRIMINALE ÇËSHTJE TË PRAKTIKËS GJYQËSORE
Magistrate Migena Laska **509 - 523**

ONLINE DRUG TRAFFICKING
Prof.Asoc. Fabian Zhilla **525 - 538**

ZBATIMI I TEKNOLOGJISË SË INFORMACIONIT NË GJYKATA
Magistrate Fatri Islamaj Ph.D. **539 - 559**

SI KA NDIKUAR TEKNOLOGJIA MODERNE NË KRYERJEN E VEPRAVE PENALE, NËPËRMJET SAJ
Ph.D. Pjereta Agalliu **561 - 583**

TEKNOLOGJIA DHE KRIMINALITETI: ROLI I KARTAVE TE KREDITIT
Ph.D. Iv Rokaj LLM & Ph.D. Teuta Hoxhaj **585 - 601**

TECHNOLOGICAL DEVELOPMENT, IMPACT ON HUMAN RIGHTS AND FREEDOMS
Ph.D. Safet Krasniqi, Ph.D. Mirvete Ukaj & M.Sc. c. Rilind Hoti **603 - 614**

DIGITAL PROFILING E CYBERCRIME, LA NUOVA FRONTIERA DEL CRIMINE
Ph.D. Enida Bozheku **615 - 631**

ROLI DHE NDIKIMI I TEKNOLOGJISË NË ZHVILLIMIN E SË DREJTËS PENALE DHE PROCEDURËS PENALE
Magistrate Olgert Rumnici & Prof.Asoc. Skerdian Kurti **633 - 645**

Panel C - Criminological Analysis and the Role of Technology in Crime Prevention

Moderator: Prof. Altin Shegani Ph.D.

LEGAL ISSUES OF CYBERSECURITY IN ELECTIONS
Ph.D. Ada Güven -Hajnaj **647 - 664**

PROTECTION OF VICTIMS FROM CRIMINAL OFFENSES BY CAUSED TECHNOLOGICALS DEVELOPMENTS
Prof.Asoc. Lirime Çukaj & M.Sc. Denisa Laçi **665 - 678**

LEGAL PROTECTION FOR INTELLECTUAL PROPERTY RIGHTS IN THE DIGITAL MARKETS: AN OVERVIEW OF THE AVAILABLE LEGAL REMEDIES AGAINST ONLINE TRADEMARK INFRINGEMENT
Ph.D. Etlon Peppo & Prof.Asoc. Jola Bode **679 - 698**

THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN PREVENTION OF CORRUPTION IN ALBANIAN JUDICIARY SYSTEM
Ph.D. Bojana Hajdini & Ph.D. Gentjan Skara **699 - 721**

TENDENCAT NË RRITJE TË DISKRIMINIMIT DHE INTOLERANCËS NËPËRMJET ZHVILLIMIT TË TEKNOLOGJISË DHE ROLI I DREJTËSISË PENALE
M.Sc. Kristina Puçi & M.Sc. Ardita Kurti **723 - 743**

WHY BITCOIN MUST BE JUST THE BIGGEST PONZI SCHEME THAT EVER EXISTED?
Magistrate Brunilda Jani Haxhiu & Ph.D. Adrian Leka **745 - 760**

NDIKIMI I TEKNOLOGJISË NË TË DREJTAT E NJERIUT
M.Sc. Marjela Peri & M.Sc. Anxhela Lalaj **761 - 775**

LIDHJA MES TË DREJTAVE TË NJERIUT DHE TEKNOLOGJISË DHE EFEKTI I TYRE NË TË DREJTAT E NJERIUT
M.Sc. Ingrida Behri Mustafa & M.Sc. Lira Spiro **777 - 794**

SHPËRNDARJA KOMPJUTERIKE E MATERIALEVE PRO GENOCIDIT OSE KRIMEVE KUNDËR NJERËZIMIT
Magistrate Elsa Miha & Magistrate Armand Gurakuqi Ph.D. **795 - 811**

PËRDORIMI I TEKNOLOGJISË NË PARANDALIMIN E AKTIVITETIT KRIMINAL TË KRIMIT TË ORGANIZUAR BRENDA SISTEMIT PENITENCIAR
Prof.Asoc. Skerdian Kurti **813 - 827**

KRIMI KIBERNETIK DHE SIGURIA KIBERNETIKE
Ph.D. Ela Kerka & M.Sc. Sonja Memoçi **829 - 845**

CËNIMI I TË DREJTËS SË AUTORIT DHE MBROJTJA E SAJ NË ASPEKTIN ADMINISTRATIV
M.Sc. Enea Sheqi & M.Sc. Ina Hasankolli **847 - 858**

PARANDALIMI DHE ZBULIMI I KRIMEVE ME MJETE TEKNOLOGJIKE
M.Sc. Arber Toci & Ph.D. Iv Rokaj LL.M. **859 - 874**

HUMAN RIGHT AND TECHNOLOGY
M.Sc. Endi Kalemaj & Prof.Asoc. Ervis Çela **875 - 888**

EDUKIMI SOCIAL NË KOSOVË PËR ZGJIDHJEN E KONTESTEVE BIZNESORE PËRMES ARBITRAZHIT
Prof.Asoc. Arif Riza & M.Sc. Fatmir Halili **889 - 899**

NECESSARY TAX AND FINANCIAL POLICIES IN TIMES OF CRISIS POLITIKAT E NEVOJSHME TATIMORE DHE FINANCIARE NE KOHË KRIZASH
Ph.D. Ejona Bardhi **901 - 913**

PEGASUS – THE GOOD, THE BAD, THE EVIL
Dr. Ivas Konini & Dr. Genada Taho **915 - 931**

NDRYSHIMET E LEGJISLACIONIT TË BE-SË MBI PARANDALIMIN E PASTRIMIT TË PARAVE LIDHUR ME PORTOFOLET ANONIME TË KRIPTO-MONEDHAVE
Prof.Asoc. Evisa Kambellari Esq. & Prof.Asoc. Engjell Likmeta **933 - 942**

CORPORATE CRIMINAL LIABILITY AND NEW TECHNOLOGIES: DIGITAL COMPLIANCE STRATEGIES IN THE FIGHT AGAINST ECONOMIC CRIMES

by EMANUELE BIRRITTERI

Adjunct Professor in European Criminal Law and Post-Doctoral Research Fellow in Criminal Law

Luiss Guido Carli University, Rome (ebirritteri@luiss.it)

Abstract:

New technologies such as artificial intelligence (AI) and blockchain are likely to change the approach to criminal compliance in corporations. Indeed, through the processing of an extraordinary amount of data and the use of digital tools organisations may identify risks and red flags that cannot be easily detected by "human analysis".

In addition, digitalisation may make internal corporate decision-making processes more transparent, so as to hinder the commission of crimes.

This way, companies may strengthen their criminal compliance systems with significant benefits in terms of meeting the regulatory requirements set by the many enforcement agencies now dealing with the fight against economic crime in the international scenario.

Nevertheless, these digital criminal compliance activities raise several issues.

On the one hand, and beyond the technical challenges, their implementation may affect regulations on remote control of workers and privacy, as well as defensive rights of individuals targeted by automated analyses when such

tools are used in the context of internal investigations.

On the other hand, the impact that these technologies may have with respect to the judicial assessment of "corporate fault" is still under-investigated (e.g., if the commission of the offence was made possible by the failure to identify a risk by the IT compliance tool).

Therefore, with a cross-cutting approach to the different domestic regulations on corporate criminal liability, this paper aims at analysing the promises, perils and future perspectives of digital compliance in this field.

Outline. 1. New technologies and criminal compliance: an introduction. 2. Overview of the main digital criminal compliance strategies implemented by corporations. 3. Technical and legal challenges. 4. Final Remarks.

1. New technologies and criminal compliance: an introduction

New technologies such as artificial intelligence (AI) and blockchain are likely to change the approach to criminal compliance in corporations.

Indeed, using digital tools organisations may identify risks and red flags that cannot be easily detected – or cannot be detected at all – by "human analysis"[1].

These IT devices process an extraordinary amount of data related to the corporation's activities, coming both from the internal organisation (i.e., the company itself) and from outside (public databases or open sources available on the Internet). These analyses aim at identifying red flags, anomalous actions and behaviour in business processes, behind which there could be illegal conduct.

Taking into account the impressive computational power of these IT solutions, it is easy to realise the great support they can provide in enabling companies to discover illegal actions committed by their employees, prevent possible criminal behaviour, understand which areas of the company need enhanced control tools, etc[2].

In addition, digitalisation may make internal corporate decision-making

1 For an in-depth analysis of these practices and a comprehensive literature review see E. Birritteri, Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri, *Diritto penale contemporaneo – Rivista Trimestrale*, 2019, n. 2, p. 289 ff.

2 See also the recent essay of G. Morgante and G. Fiorinelli, Promesse e rischi della compliance penale digitalizzata, *Archivio Penale*, 2022, n. 2, p. 2 ff.

processes more transparent, so as to hinder the commission of crimes.

The reference is here, above all, to the 'migration' of certain decision-making processes of the corporation within a blockchain architecture, which can allow to make the data stored in it fully visible and unchangeable. Even in such a decision-making system, of course, it can be very risky to commit a crime, as the chance of being caught increases significantly for an employee[3].

This way, using all these tools, companies may strengthen their criminal compliance systems with significant benefits in terms of meeting the regulatory requirements set by the many enforcement agencies now dealing with the fight against economic crime in the international scenario.

The evaluation of a corporation's ability to build a good compliance and internal controls system to prevent unlawful conduct is indeed an important feature of all major corporate criminal liability models, although the positive outcome of such an assessment may have different effects in terms, as the case may be, of exemption from any liability or simply a reduction of sanctions or the granting of access to negotiated settlements[4].

Nevertheless, these digital criminal compliance activities raise several issues.

On the one hand, and beyond the technical challenges, their implementation may affect regulations on remote control of workers and privacy, as well as defensive rights of individuals targeted by automated analyses when such tools are used in the context of internal investigations[5].

On the other hand, the impact that these technologies may have with respect to the judicial assessment of "corporate fault" is still under-investigated (e.g., if the commission of the offence was made possible by the failure to identify a risk by the IT compliance tool)[6].

Therefore, with a cross-cutting approach to the different domestic regulations on corporate criminal liability, this paper aims at analysing the promises, perils and future perspectives of digital compliance in this field.

The research will be divided into three sections.

3 A. Gullo, voce *Compliance*, *Studi in onore di Carlo Enrico Paliero* (forthcoming).

4 For a comparative study on corporate criminal liability see, among others, M. Pieth and R. Ivory (eds), *Corporate Criminal Liability. Emergence, Convergence, Risk*, Springer, London-New York, 2011; see also the recent monograph of R. Sabia, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Giappichelli, Torino, 2022.

5 See paragraph 3.

6 See paragraph 3.

In the first part, we will provide a brief overview of the main digital criminal compliance tools adopted by corporations today.

In the second section, we will focus on the technical challenges and legal issues related to the use of such systems.

Finally, in the last part, we will make some remarks on the main strengths and weaknesses of these strategies as well as on the future perspectives of the phenomenon.

2. Overview of the main digital criminal compliance strategies implemented by corporations

One of the main digital criminal compliance strategies implemented by corporations involves the use of big data analytics tools and artificial intelligence software in general to analyse data[7].

Nowadays, private companies (especially large ones) must deal with a considerable amount of heterogeneous data produced in real time.

This type of data (which are often called big data, whose characteristics are highlighted by the so-called 3 Vs: volume, variety, velocity) cannot be managed through traditional methods of analysis but requires the help of new technologies.

These technologies show that it is possible to transform aseptic data into relevant information for the management and prevention of corporate criminal risk[8].

Therefore, automated IT tools have been implemented for the analysis – also through the use of artificial intelligence algorithms and software – of significant amount of data: these data may belong to the company or be freely accessible on the web or in certain databases (e.g., public procurement databases etc.).

7 G. Morgante and G. Fiorinelli, Promesse e rischi della compliance penale digitalizzata, cit., p. 9 ff.

8 L. D'Agostino, *Criminal compliance e nuove tecnologie*, Pubblicazione CRUI (forthcoming). For a broader analysis on the links between artificial intelligence and criminal justice see also F. Basile, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, *Diritto penale e uomo*, 2019, p. 2 ff. The importance of digital tools in preventing and combating crimes has been also recognised by the OSCE Decision no. 6/20 on Preventing and Combating Corruption Through Digitalization and Increased Transparency (OSCE Ministerial Council, Tirana, 2020). See also, on this topic, the papers published in the *Revue Internationale de Droit Pénal*, 2021, in the issue edited by G. Vermeulen, N. Persak and N. Recchia on the topic *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*.

These analyses have three main purposes:

1) identifying red flags and warning signs in the company's operations (in particular, anomalous actions with respect to behaviour patterns that the system qualifies as recurrent/ordinary);

2) e-mail traffic monitoring, in order to identify conversations in which certain keywords considered to be "at risk" are used;

3) provide management with a real-time report on any red flags in the behaviour of (or in the data collected on) the partner/agent with whom certain transactions are in progress (so-called third-party due diligence)[9].

Such systems compare different data, through the extraordinary computational capabilities of the digital software that they use and are able to find connections and links between information/data that a human being would often not be able to find.

These tools can identify many red flags and warning signals, including, for example:

1) purchase prices, consultancy fees and cash flows that are anomalous with respect to the average reference price in the business sector and geographical area;

2) possible conflicts of interest between the members of the corporate functions involved in the transactions and third parties;

3) suspicious financial movements with respect to the entity's business 'history'[10].

Obviously, when such software reports these red flags, this does not necessarily mean that a crime has been committed, but only that it is necessary to deepen the case and investigate further in order to understand whether illegal behaviour or simply some issues of disorganisation lie behind this anomaly.

However, this activity is also useful to understand in which branches of the corporation the preventive and control measures need to be strengthened.

Another relevant digital criminal compliance strategy is to promote the 'migration' of certain decision-making processes of the corporation within a

9 See, also for other references, E. Birritteri, Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri, cit., p. 290.

10 E. Birritteri, Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri, cit., p. 291.

blockchain architecture[11].

Indeed, certain studies have highlighted that it is possible to build a blockchain system with a central governing body (the company's management) and various "nodes" of the chain located in the organisational and decision-making structure of the corporation. The "nodes", in particular, would be also the various control bodies of the corporation (e.g., supervisory body etc.).

In this way, the decision-making process of the corporation would take place within the blockchain architecture, guaranteeing:

1) the "unchangeability" of the data and thus the full transparency of operations;
2) the possibility of automatically triggering, by means of smart contracts, the crime prevention policies set by the management, with the option, moreover, of integrating this blockchain architecture with the aforementioned data analytics systems[12].

Such an innovation, of course, would greatly enhance the corporation's criminal compliance strategy, since, notwithstanding it would be very difficult for an individual to commit an offence within such a decision-making system, crime prevention policies would be automatically implemented in this structure built to operate, "by design", in accordance with the compliance strategies decided by the organisation's top management.

3. Technical and legal challenges

There are no (direct) public regulations of these phenomena related to the implementation of digital criminal compliance strategies.

This leads to a few challenges and issues on both a technical and legal level.

With regard to technical aspects, the absence of any direct public regulation of these practices means that it is up to the individual corporation to decide how to build the system, which surveys to carry out or not to carry out, which data to use or not to use.

This raises a first issue related to the quality and reliability of such digital

11 A. Gullo, voce *Compliance*, *Studi in onore di Carlo Enrico Paliero* (forthcoming).

12 For an analysis of this topic, see, also for a broader literature review, G. Soana, Corporate Compliance Integrata e Blockchain, in L. Luparia and G. Vaciago (eds.), *Compliance 231. Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore*, Gruppo24Ore, Milano, 2022, p. 321 ff.

analyses.

Indeed, the quality and reliability of the result of such digital surveys can only depend on a series of factors including:

1) the quality, reliability and above all the completeness of the data used by the software;
2) the way in which the survey is designed and implemented, especially in terms of the level of detail of the investigations.

In short, if the data are collected in a partial manner or from unreliable sources, or if the investigation, although using reliable data, is not carried out in a detailed and exhaustive manner, the result of such assessments will not be trustworthy.

These tools, indeed, can only identify useful and reliable red flags – and can really strengthen a corporation's compliance system – if from a technical point of view they are based on complete and accurate surveys and data[13].

Another issue is that several times there is a lack of communication between private data and public database (of prosecutors, public procurement authorities, etc.).

This is of course another key point, because very often the most reliable data (or at least those that are most useful for carrying out analyses aimed at preventing illegal conduct) are managed directly by public administrations and several times are not (at least fully) accessible by companies. The lack of access to many of these data, then, makes it more complex to carry out a digital survey of this kind that aims to be as reliable as possible[14].

In addition to the technical challenges, there are also several legal issues.

In fact, although the ultimate aim of these investigations is to prevent illegal behaviour within private businesses – and thus, from the perspective of corporations, to avoid sanctions and comply with corporate criminal liability regulations – there is a rather tangible risk that, in trying to comply with the laws at stake using these instruments, corporations will violate other regulations.

These are, in short, activities that, while aimed at avoiding risks for

13 See the CEPEJ *European Charter on the use of Artificial Intelligence in judicial systems and their environment*, p. 10. For an analysis of this charter see S. Quattrocolo, Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche, *La legislazione penale*, 18 December 2018.

14 E. Birritteri, Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri, cit., p. 292.

companies, may generate additional and different legal risks – we might say, of a secondary or indirect nature – from those that they aim to contain and manage.

One of the main issues is whether privacy protection laws can be applied to these types of digital compliance activities[15].

In order to answer this question, it is necessary to understand whether or not the data analysed by these digital tools can be considered personal data, since most privacy regulations, such as the General Data Protection Regulation (GDPR) in the European context, can only apply when it comes to personal data (i.e., data referring to a specific individual).

At first glance, we might answer no to this question, considering that these IT investigations, at least in most cases, analyse aggregate (corporate) data, relating in general to the overall business and company operations that are being or have already been carried out in that organisation – and thus not directly linked to data of a specific individual.

However, it cannot be ruled out in general that, in specific cases, the use of such tools may entail the need to process personal data, nor can it be excluded that, at the end of the IT investigation of aggregated business data, the need to process information relating to a specific individual emerges at a second stage (e.g., when the red flag reported by the system relates to a deal managed directly by a single employee).

By virtue of a concept known as the privacy by design principle (recognised for instance by regulations such as the GDPR), this possibility of tracing individuals through the IT investigation makes it necessary to structure – before starting to use the digital compliance software – measures to protect the privacy rights of those involved in the software investigation[16].

One of the most important of these privacy rights is the right to human intervention in cases of automated data processing (and of course, the digital systems we have mentioned can in many cases be considered as such, since the analysis of information is carried out autonomously by the software)[17].

The basic idea behind this right is that in situations where a certain decision on an individual (e.g., concerning the employee's professional liability) is based, as is often the case here, on automated data processing, the result of

15 R. Sabia, Artificial Intelligence and Environmental Criminal Compliance, *Revue Internationale de Droit Pénal*, 2020, p. 193.

16 R. Sabia, Artificial Intelligence and Environmental Criminal Compliance, cit., p. 194.

17 On this topic see G. Ubertis, Intelligenza artificiale, giustizia penale, controllo umano significativo, *Diritto penale contemporaneo – Rivista Trimestrale*, 2020, n. 4, p. 75 ff.

the IT software cannot be the only element in making the final choice, but it must be part of a broader assessment carried out by a human being[18].

Moreover, the recognition of this right also implies that it must be ensured that the employee or the person involved in such investigations is able to know how the software works and to challenge the result produced by the digital tool (and this can be very difficult too, because very often such instruments are based on the use of sophisticated algorithms whose functioning is not fully known even by the programmers/creators of the device)[19].

The violation of these rules on the protection of privacy of course often entails the application of sanctions (one can mention, for example, the considerable fines provided for by the GDPR).

In short, an activity by which the corporation seeks to avoid corporate criminal liability sanctions is likely to lead to the application of different punitive measures, if not properly carried out in view of the possible application of such regulations designed for other cases but, as seen, applicable to such digital investigations.

Another legal issue concerns the enforcement of laws protecting workers' rights[20].

Indeed, in many legislations, the use of these devices can be qualified as a form of remote control on the activity of workers.

As a consequence, this would imply the application of the rules protecting employees' rights, with particular reference to the guarantees to be granted to them with respect to instruments for the control of their operations.

Therefore, in order to use these systems a company may have to comply with these labour law regulations, for example reaching a prior agreement with the trade union or, failing that, a prior authorisation from the competent labour inspectorate. Moreover, under several jurisdiction the company must provide workers with adequate information (their consent is often not required) on the way in which the IT software it is used and the way in which the surveillance is carried out (this is, for instance, what happens in

18 G. Ubertis, Intelligenza artificiale, giustizia penale, controllo umano significativo, cit., p. 75 ff. See also M. Gialuz, Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa, *Diritto penale contemporaneo*, 29 May 2019.

19 For a broader analysis of this issue see M. Mozzarelli, Digital Compliance: The Case for Algorithmic Transparency, in S. Manacorda and F. Centonze (eds.), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer, Cham, 2022, p. 259 ff.

20 See, for an in-depth investigation of this topic, A. Nisco, Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normative e tecnologico, *Diritto penale contemporaneo – Rivista Trimestrale*, 2021, n. 4, p. 87 ff.

the Italian jurisdiction, where failure to comply with all these rules may result in a criminal sanction)[21].

On the other hand, the case where there is already a definite suspicion of unlawful or criminal acts being carried out by the employee is different: regardless of *ex ante* compliance with the aforementioned rules in question, in fact, in such cases prior information to the employee would compromise the need for secrecy and speed of the internal investigation necessary to protect the interests of the company. Therefore, case law has clarified that in such cases the employer can carry out a covert control but just to assess if there are offences in progress and not to install a remote surveillance system on a regular basis without complying with these regulations[22].

Here too, then, the use of such digital compliance tools, aimed at preventing the corporation from being subject to the various regulations relating to corporate criminal liability, is likely to lead to the possible application of other sanctions.

A further legal issue, then, is that of the interplay between these digital criminal compliance strategies, corporate internal investigations and the defence rights of those involved in such IT analyses, also because the practices under analysis could themselves become one of the tools through which the organization can carry out its own internal investigations[23].

Using this type of automated software in criminal compliance, indeed, evidence concerning the criminal liability of certain individuals may be identified.

This clearly requires defining the system of procedural safeguards – for instance with respect to the issue of self-incrimination – to be recognized to the persons involved, especially in view of the fact that – apart from the cases in which such investigations can be qualified as defensive investigations

21 See also, among others, G. Proja, Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza, *Rivista italiana di diritto del lavoro*, 2016, n. 4, p. 547 ff., and L. Tebano, Employees' privacy and employers' control between the Italian legal system and European sources, *Labour & Law Issues*, 2017, vol. 3, n. 2, p. 1 ff.

22 See, also for detailed references to the relevant case law (with particular regard to the ECHR's case Lopez Ribalda Vs Spain, 17 October 2019), E. Birritteri, Controllo a distanza del lavoratore e rischio penale, *Sistema penale*, 16 Febraury 2021.

23 On the topic of corporate internal investigations see among others: E.M. Mancuso, Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte, in F. Centonze and M. Mantovani (eds.), *La responsabilità «penale» degli enti. Dieci proposte di riforma*, Il Mulino, Bologna, 2016, p. 217 ff., and A. Nieto Martin, Internal Investigations, Whistle-Blowing and Cooperation: The Struggle for Information in the Criminal Process, in S. Manacorda, F. Centonze and G. Forti (eds.), *Preventing Corporate Corruption: The Anti-Bribery Compliance Model*, Springer, London, 2014, p. 69 ff.

under the criminal procedure code – in several jurisdiction (for example in Italy) there is no legislative regulation for these corporate investigation activities, which are often carried out before or regardless of the existence of a criminal proceeding and by professional without the formal qualification of lawyers[24].

The protection of the defence rights of employees or in general of persons affected by such digital investigations, then, is still an open issue.

Finally, a further legal problem could arise with reference to the application of those models of corporate criminal liability based on organisational fault or in any case on the "failure to prevent" system.

In these types of corporate criminal liability laws, indeed, the entity is punished by virtue of an organisational failure, often assessed with regard to the adoption of a compliance program or adequate procedures to prevent the offence from being committed[25].

It is, therefore, a fault directly related to the activities of the corporation as such.

The use of these digital criminal compliance systems, then, could generate additional problems in terms of assessing this organisational fault, especially in cases where the failure to prevent the crime committed in the interest or to the advantage of the corporation is due to a malfunction of a digital compliance device that the legal person merely uses, without having produced or created it[26].

Is it possible in such cases to prove the organisation's fault? If so, does this fault lie in the fact that, from the outset, the corporation decided to rely entirely on such IT models to prevent crimes, or in the fact that the company units in charge did not check the reliability of the investigation carried out by the IT tool?[27]

24 See F. Nicolicchia, Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della "lezione americana", *Rivista trimestrale di diritto penale dell'economia*, 2014, n. 3-4, p. 781 ff.

25 See, also for a wide international literature review on this topic, R. Sabia, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Giappichelli, cit., *passim*.

26 See also A. Nisco, Riflessi della compliance digitale in ambito 231, *Sistema penale*, 14 March 2022, and R. Sabia, Artificial Intelligence and Environmental Criminal Compliance, cit., p. 194 ss. In general, with respect to the strengths and weaknesses of digital criminal compliance see also V. Mongillo, Presente e future della compliance penale, *Sistema penale*, 11 January 2022 and P. Severino, The Importance of Corporate Compliance in the Digital Era, *Revue Internationale de Droit Pénal*, 2020, p. 435 ff.

27 See also Nicola Selvaggi, *Compliance, sicurezza informatica e nuove tecnologie*, Text of the

There are therefore several open issues from this perspective as well, and indeed it is difficult to assume that it is possible to prove an organisational fault of the corporation without somehow being able to identify a fault of one of its managers or employees with respect to the use of such IT tools.

4. Final Remarks

Are we moving from a criminal compliance system that rely upon classic human activities of analysis and preventive investigation 'in the field', to a fully automated model in which it is the "machine" alone that takes upon itself the role of assessing the criminal risk and identifying the procedures to manage it – and in which the human being only has the task of ensuring that the IT software has sufficient "fuel reserves" (i.e., data) to be able to carry out its surveillance tasks?

Perhaps it is still too early to raise such a question.

We are not yet facing such a "tragic alternative" between two conflicting models, between "analogical" and "digital" compliance.

It is more likely that we will move more and more towards a "mixed system", where criminal compliance will continue to rely and must necessarily rely upon human input, but where new technologies will play an increasingly important role.

Therefore, we have to try to understand, in this final section of the research, which are the main strengths and weaknesses associated with the implementation of these digital criminal compliance strategies, as well as the future perspectives with respect to the use of these systems to prevent crimes in the context of private organisations.

Certainly, the main benefits that these tools provide are related to the strengthening of the overall reliability and effectiveness of the criminal compliance and internal control systems designed and implemented by the corporation.

Indeed, these practice could be qualified as data-driven criminal risk management strategies, in which the decisions taken by the corporation on the type of controls to be performed and the preventive measures to be adopted to prevent crimes would not be based on a generic (human) analysis of the characteristics of that particular economic activity, but on an in-depth examination of any relevant corporate data, carried out by an advanced IT

speech given at the Congress of the International Association of Penale Law – Italian Group (Teramo, Italy, 22-23 March 2019, forthcoming).

tool capable of linking different data (coming from the company's operations as well as from public databases/open sources) and finding connections between information that a human being would simply not be able to identify.

These strategies, in short, would strengthen both the risk assessment and risk management phases, of course assuming that from a technical point of view the IT analyses are well designed and implemented and, above all, based on a comprehensive database of reliable and verified information.

On the one hand because the corporate's compliance program would be built on the basis of a risk analysis carried out through a pervasive survey, and with the extraordinary computational capabilities of the IT software, of the entire corporate information assets.

On the other hand, because these systems can be used not only during risk assessment but also as concrete prevention tools/procedures (for example with respect to third party due diligence), in order to automatically verify that every use of company assets is carried out in compliance with the crime risk prevention policies imposed by company management.

In this respect, then, the use of such tools can bring various benefits to the corporation; in fact, according to the relevant applicable model of corporate criminal liability, having designed and implemented an effective compliance system (which, as we have seen, the use of IT tools can significantly improve) can exempt the corporation from liability, or lead to a reduction of sanctions, or allow the corporation to enter a negotiated settlement with the public prosecutor.

From a different perspective, however, we have also seen that the use of these systems can also entail various risks for the corporation or, in general, several legal problems that are still open issues.

Indeed, on the one hand, corporations may be sanctioned for the use of such systems if they fail to check if the way in which they are designed and applied complies in particular with the regulations on the protection of privacy and the remote control of employees' activities.

On the other hand, and in general, there are several concerns regarding both the protection of the procedural rights of defence of those involved in such investigations, and the possibility that potential liability gaps may arise with respect to the assessment of the organisational fault of corporations.

Moreover, at least according to some scholars, one of the main risks associated with the implementation of these digital criminal compliance strategies is that of legitimising a kind of "surveillance capitalism", in which employees are considered as sources of possible legal risks for the company

and must therefore be constantly monitored, through a pervasive "cyber-tracking" of their activities to prevent any possible illegal conduct[28].

Our contention, however, is that it is a mistake to adopt a drastic approach to this issue, both when it comes to allowing a totally unregulated use of tools that may in several cases affect fundamental rights of the individual, as well as in terms of a radical rejection of every possible benefit that technology can bring even in the area of criminal compliance.

The future goal to be pursued, especially with regard to the role of public decision-makers, must be to establish a direct regulation of the phenomenon, in particular by specifying which are the best practices that a company can/must adopt if it wishes to use these digital criminal compliance tools, which may also be very useful in the future with regard to reporting activities and cooperation with enforcement authorities[29].

It is clear, indeed, that it is not possible, through the implementation of regulations on corporate criminal liability, to ask companies to play a proactive role in crime prevention, thus exercising a function that is normally under the responsibility of public actors, and at the same time sanction those organisations that invest considerable resources in designing cutting-edge tools in fulfilling this particular task.

It is necessary, then, to effectively balance the various interests and rights at stake, through a public regulation that clarifies the measures and precautions that businesses must adopt in order to benefit from the advantages associated with the use of digital criminal compliance instruments, without leaving behind the protection of fundamental rights of those affected by such investigations.

28 C. Burchard, L'inteligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società, *Rivista italiana di diritto e procedura penale*, 2019, p. 1909 ff. For an in-depth analysis of the issues related to the evolution of compliance in these areas see also W.S. Laufer, The Missing Account of Progressive Corporate Criminal Law
, *New York University Journal of Law & Business*, 2017, vol. 14, n. 1, p. 71 ff.

29 For a broader analysis see E. Birritteri, Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri, cit., p. 297 ff.

PËRDORIMI I TEKNOLOGJISË, VIKTIMAT E KRIMIT DHE TË DREJTAT E SAJ NË SISTEMIN E DREJTËSISË PENALE NË SHQIPËRI

PROF. DR VASILIKA HYSI

Pedagoge me kohë të pjesshme
Fakulteti i Drejtësisë, Universiteti i Tiranës

hysi.vasilika@gmail.com

Abstrakt

Zhvillimet teknologjike po ndikojnë gjithnjë e më shumë në të gjitha fushat e jetës. Teknologjia gjen zbatim të gjerë në menaxhimin e sistemit të drejtësisë, përfshirë drejtësinë penale. Përdorimi i saj ndikon në forcimin e bashkëpunimit ndërkombëtar penal, zbulimin e krimeve, në mbledhjen e provave, sigurinë e jetës së viktimave dhe dëshmitarëve, në mbrojtjen dhe garantimin e të drejtave të njeriut në sistemin e drejtësisë penale. Nga ana tjetër, teknologjia ka ndikuar në shfaqjen e formave të reja të kriminalitetit, lehtëson kryerjen e veprave penale, sidomos të krimeve ekonomike, krimit të organizuar, krimit kompjuterik ose akteve terroriste. Teknologjia mundëson jo vetëm forma më të sofistikuara të krimit, por edhe mbulim të gjurmëve dhe provave të tij.

Parandalimi i krimit, luftimi i krimit të organizuar dhe mbrojtja e viktimave, sidomos grave dhe fëmijëve ishin pjesë e reformës në drejtësi të ndërmarrë gjatë viteve të fundit në Shqipëri. Bërja drejtësi për fëmijët dhe për viktimat, ka diktuar nevojën e masave mbrojtëse për ta, para fillimit të procedimet, gjatë dhe pas përfundimit të tij. Garantimi i sigurisë gjatë procesit penal, dhënia e dëshmisë nëpërmjet përdorimit të teknologjisë audio video dhe sistemit vidiokonferencë në procedimet penale është një nga orientimet e politikës penale shqiptare. Trajtimi i viktimave, bazuar në

nevojat e saj, sidomos të viktimave të krimit të organizuar, dhunës në familje mbetet ende një sfidë në drejtësinë penale shqiptare.

Në këtë kumtesë trajtohen ndikimi i teknologjisë në mbrojtjen e viktimave të krimin, veçanërisht fëmijët viktimë me qëllim sigurinë e tyre; bëhet një vlerësim empirik i evoluimit të politikës penale për mbrojtjen e vitimës nëpërmjet përdorimit të teknologjisë, efektivitetit të saj dhe sfidave që hasen në praktikë. Gjithashtu, trajtohet respektimi i të drejtave të njeriut kur përdoret teknologjia në procedimet penale. Disa gjetje dhe përfundime paraqiten në fund të kumtesës.

Fjalë kyçe

Teknologji, procedim penal, viktima, të drejtat e viktimës, sistemi video dhe audiokonferencë.

1. Përdorimi i teknologjisë, krimi dhe sistemi i drejtësisë penale

Çdo ditë e më shumë kriminaliteti, veçanërisht krimi i organizuar, trafikimi, shfrytëzimi për prostitucion, terrorizmi, shkaktojnë viktima të shumta. Gratë, vajzat, fëmijët, të huajt janë grupe më të riskuara. Teknologjia përdoret për të kryerjen e krimeve ose për të fshehur gjurmët e tyre, sidomos për krimet financiare, kibernetike, kompjuterike, krimin e organizuar, përfshirë trafikimin e qënieve njerëzore për qëllime të ndryshme, shfrytëzim prostitucioni, pedofili etj. Trafikantët dhe autorët e tjerë të krimeve përdorimin teknologjinë për të identifikuar dhe tërhequr në krim viktimat e tyre.[1] Nga ana tjetër, teknologjia po përdoret gjërësisht për zbulimin e krimeve, të krimit të organizuar, trafikimit[2] dhe në proceset penale. Përdorimi i provave online që gjenden në telefonat smart, rrjetet sociale, instragram, etj ndihmojnë zbulimin e asaj çfarë ka ndodhur dhe mbrojnë viktimat/ viktimat e mundshme të krimit. Pasja e një mjedisi të

1 Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies, Donna M. Hughes, botuar në SAGE Open Volume 4, Issue 4, October-December 2014. Shih: https://journals.sagepub.com/doi/epub/10.1177/2158244014553585. Dokumenti u aksesua në datën 8 gusht 2022.

2 Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons, UN, 2021. Shih: https://www.unodc.org/documents/treaties/WG_TiP_2021/CTOC_COP_WG.4_2021_2/ctoc_cop_wg.4_2021_2_E.pdf. Dokumenti u aksesua në datën 8 gusht 2022.

sigurt dhe pjesëmarrja e viktimës në procesin penal, pa u përballuar me autorin e saj mundësohen gjithashtu nga teknologjia.

Teknologjia po përdoret gjerësisht për menaxhimin e sistemit të drejtësisë. Transformimi dixhital i sistemit të drejtësisë, përdorimi i teknologjisë, sidomos i inteligjencës artificale janë arritje, por nga ana tjetër, është rritur shqetësimi në lidhje me respektimin e të drejtave të njeriut në sistemin e drejtësisë dhe në fushat e tjera ku inteligjenca artificiale ka gjetur përdorim.[3] Për këtë arsye, gjatë dekadës së fundit institucionet ndërkombëtare, përfshirë BE-në dhe Këshilli i Evropës (KE) kanë miratuar rekomandime dhe strategji për përdorimin e teknologjisë dhe sidomos inteligjencës artificiale.[4] Bashkimi Evropian (BE)[5] po diskuton masa dhe instrumente që mund të zbatohen për transformimin dixhital të sistemeve të drejtësinë në vendet anëtare të BE-së dhe brenda institucioneve të saj. Qëllimi është modernizimi i sistemeve të drejtësisë, i gjykatave në veçanti, lehtësimi e aksesit te shërbimet e drejtësisë, dosjet e çështjeve, lehtësimi i komunikimit mes palëve dhe administratës gjyqësore.

Dixhitalizimi i bashkëpunimit ndërkombëtar në çështjet penale është një hapësirë e përdorimit të teknologjisë që ka ardhur duke u rritur. Përdorimi dhe pranimi i nënshkrimit elektronik, transmetimi elektronik i kërkesave në një një kohë të shkurtër dhe në mënyrë të sigurt në kuadër të bashkëpunimit ndërkombëtar, provat online, përdorimi i vidiokonferencave për marrjen e dëshmive kur personi gjenden jashtë vendit ose nuk mund të jetë i pranishëm fizikisht për të dëshmuar në polici, prokurori ose gjykatë janë falë zhvillimeve të teknologjisë.[6]

3 Përdorimi i gjerë i intelegjencës artificiale, përparësitë dhe risqet e saj në raport me respektimin e të drejtave të njeriut nuk trajtohen në këtë kumtesë.

4 Shih: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU Policy Paper. Shih: https://www.ceps.eu/wp-content/uploads/2021/05/Criminal-Justice-Fundamental-Rights-and-the-Rule-of-law-in-the-Digital-Age.pdf dhe Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Këshilli i Evropës, miratuar më 8 Prill 2020. Shih: https://rm.coe.int/09000016809e1154. Dokumenti i aksesua më datë 8 Gusht 2022.

5 Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age, Sergio Carrera Valsamis Mitsilegas Marco Stefan, botim i Centre for European Policy Studies (CEPS), Brukse, Maj 2021. Shih: https://www.ceps.eu/wp-content/uploads/2021/05/Criminal-Justice-Fundamental-Rights-and-the-Rule-of-law-in-the-Digital-Age.pdf. Dokumenti është aksesuar në datën 8 Gusht 2022.

6 Manual on Videoconferencing Legal and Practical Use in Criminal Cases, UN, New Yourk,2017.Shih:https://www.unodc.org/documents/organized-crime/GPTOC/GP_TOC2/MANUAL_VIDEOCONFERENCING.pdf.Dokumenti u aksesua në datë 8 Gusht 2022.

Studimet[7] tregojnë përpjekjet për zgjerimin e përdorimit të teknologjisë në programet e drejtësisë restauruese, duke vënë në pah përparësitë dhe kufizimet e përdorimit të saj në programet e ndërmjetësimit viktimë-autorë.

Teknologjia po gjen zbatim në menaxhimin e sistemit të drejtësisë edhe në Shqipëri. Sipas studimeve të kryera, pjesa më e madhe e gjykatave të shkallës së parë dhe apelit në Shqipëri përdorin teknologjinë për të regjistruar audio dhe vidio seancat gjyqësore.[8] Një studim tjetër për përdorimin e sistemeve digjitale në gjykata[9] vë në pah lehtësitë në funksionin e tij, si sigurimi i regjistrimit audio dhe vidio të seancave, ndjekja e tyre dhe aksesi i palëve në regjistrimet, por edhe sfidat.[10]

Megjithë përparësitë e përdorimit të teknologjisë në drejtësinë penale, studimet vënë në pah risqe të shumta në lidhje me të drejtave e njeriut, procesin e rregullt ligjor, mbrojtjen e të dhënave personale, etj.[11] Funksioni i sistemit dhe ruajtja e regjistrimeve nga sulmet kibernetike, dëmtimet, vjetërimi i teknologjisë kërkojnë investime në infrastukturë, teknologji, përditësim, rritje të kapaciteteve të stafit IT-së dhe personel gjyqësor të

7 Is computer-based communication a valuable addition to victim-offender mediation? A qualitative exploration among victims, offenders and mediators, victims & offenders, Florian Bonensteffen, Sven zebel & Ellen Giebels publikuar në Victims & Offenders An International Journal of Evidence-based Research, Policy, and Practice, Routledge, Janar 2022. Shih: https://doi.org/10.1080/15564886.2021.2020946. Dokumenti u aksesua në datën 8 Gusht 2022.

8 Zbatimi i sistemit të menaxhimit të çështjeve civile/penale (CCMIS/ICMIS) pranë gjykatës së rrethit gjyqësor Tiranë, Durrës dhe Elbasan, raport monitorimi, ALTRI, 2018, f.18-19. Sipas raportit deri në vitin 2018 ky sistem ishte në përdorin në 2/3 e gjyatave të shkallës së parë dhe të apelit. Shih: https://altri.al/wp-content/uploads/2018/05/Raport-Monitorimi-mbi-zbatimin-e-sistemit-CCMIS-ICMIS-1.pdf. Dokumenti u aksesua në datën 18 Qershor 2022.

9 Raport mbi gjetjet e monitorimit të përdorimit të sallave të gjyqit dhe sistemit të regjistrimit digjital audio në gjykata, raport i Komitetit Shqiptar tw Helsinkit, Tiranw 2017.Shih:https://ahc.org.al/wp-content/uploads/2017/08/Raport-RDAcmyk_ValmiraOK-1.pdf. Dokumenti u aksesua në datën 8 gusht 2022

10 Aplikimi i Sistemit të Regjistrimit Dixhital Audio (RDA) në gjykatat shqiptare përbën një ndryshim thelbësor në mënyrën se si zhvillohen seancat gjyqësore, si dhe një hap të madh përpara për sa i përket transparencës dhe procesit të rregullt ligjor në Shqipëri. Gjithashtu, periudha e pandemisë e shkaktuar nga COVID 19 dëshmoi rolin e teknologjisë në vijimin e funksionimit të sistemit të drejtësisë. Disa procedura që kërkonin prezencë fizike u u kryen online.

11 Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age, Sergio Carrera Valsamis Mitsilegas Marco Stefan, vep.e cit., fq.32-36.

trajnuar që i përdor ato.[12]

Në kuadrin e një kumtesë nuk mund të trajnohet në të gjitha problemet që sjelle përdorimi i teknologjisë në procesin penal, por do të ndalemi te përdorimi i teknologjisë në procesin penal kur fëmija ku ka fëmijë në kontakt me drejtësinë. Kjo çështje trajtohet nga këndvështrimi ligjor dhe zbatimin te teknologjisë në praktikë.

2. Drejtësia penale, viktimat dhe teknologjia

Zbulimi dhe hetimi i krimeve, siodmos formave të rënda të tij, të krimit të organizuar ka nevojë për dëshminë e dëshmitarëve dhe viktimës/ave për të hedhur dritë mbi atë që ka ndodhur. Jo në pak raste, jeta e viktimës ose e dëshmitarit dhe e familjarëve të tyre vihet në rrezik nga dëshmia dhe ajo që ta kanë parë. Nga ana tjetër, viktima dhe garantimi i të drejtave të saj në procesin penal nuk janë gjithnjë në vëmendje të drejtësisë. Grupi i ekspertëve të nivelit të lartë pranë Komisionit të Posaçëm Parlamentar për Reformën në Sistemin e Drejtësisë, në analizën e sistemit të drejtësisë në Shqipëri (2015), vinte në dukje se, përveç të dëmtuarve të parashikuar nga nenet 59 dhe 284 të Kodit të Procedurës Penale (KPP), pozita procedurale e të dëmtuarit nga vepra penale ishte e dobët. Para ndryshimeve të miratuara në KPP në vitin 2017, mungesa e rregullimit ligjor dhe detajimit të të drejtave dhe garancive procedurale, në përputhje me standardet minimale të direktivës së BE u evindetuan. Raporti vinte në pah ndër të tjera, mungesën e parashikimit të mekanizmave për mbrojtjen fizike të të dëmtuarve dhe familjeve të tyre; mbrojtjen e dinjitetit të tyre gjatë pyetjes, shmangien e kontaktit të drejtpërdrejtë ndërmjet viktimës dhe të pandehurit. Sipas raportit për të dëmtuarin/viktimën e mitur nuk janë të detajuara garancitë procedurale si: shmangia e përhapjes në publik e të dhënave për identifikimin e një viktime/të dëmtuari të mitur, regjistrimi audio-video i pyetjes së të miturit dhe paraqitja si provë në gjykim e regjistrimit, etj.[13]

Bazuar sa më sipër, të drejtat e viktimës dhe garantimi i tyre në procesin penal u bënë pjesë e reformës së drejtësisë penale. Legjislacioni i miratuar si Kodi i Drejtësisë Penale për të Miturit, ndryshimet në Kodit Penal (KP), Kodin e Procedurës Penale (KPP) dhe ligjet e tjera në fushën penale ose të

12 Për më shumë shih: Raport mbi gjetjet e monitorimit të përdorimit të sallave të gjyqit dhe sistemit të regjistrimit digjital audio në gjykata, vep.e cit., fq.55-56.

13 Analiza e Sistemit të Drejtësisë në Shqipëri, Kuvendi i Shqipërisë, Qershor 2015, fq.149-150. Shih: http://www.reformanedrejtesi.al/sites/default/files/dokumenti_shqip.pdf. Dokumenti u aksesua në datën 18 Qershor 2022.

lidhur me të rregulluan më mirë të drejtat e viktimës në çdo fazë të procesit penal. Një strukturë e posaçme për të mbështetur viktimat u krijua pranë çdo prokurorie të rrethit gjyqësor me juridiksion të përgjithshëm[14] dhe një seksion i veçantë për të asistuar viktimat dhe dëshmitarët që bashkëpunojnë me drejtësië është krijuar pranë prokurorisë për luftimin e krimit të organizuar dhe korrupsionit në Shqipëri[15]. Garancitë procedurale për fëmijët në kontakt/konflikt me ligjin dhe viktimat në tërësi u bazuan në aktet ndërkombëtare ku shteti shqiptar është palë, në rekomandimet, udhërrëfyes, dokumente strategjikë, duke mbajtur parasysh mundësitë që ofron zhvillimi i teknologjisë dhe sektori privat në ditët tona.

Megjithatë, bërja drejtësi për viktimat dhe drejtësia për fëmijët përballet me sfida që ende nuk janë kapërcyer në praktikë. Përdorimi i teknologjisë me përparësitë dhe risqet që mbart është një prej sfidave. Kërkimet shkencore në këtë fushën e përdorimit të teknologjisë në sistemin e drejtësisë janë në fillimet e tyre. Në punën e bërë për përgatitjen e kësaj kumtese një nga kufizimet e hasura është literatura e kufizuar në lidhje me këtë çështje në Shqipëri, mungesa e vlerësimeve shkencore për përdorimin e teknologjisë në drejtësinë penale në tërësi dhe atë për të mitur në veçanti. Ndonëse nevoja e përdorimit të teknologjisë gjatë periudhës së pandemisë të shkaktuar nga COVID- 19 nxiti rritjen e vëmendjes së institucioneve monitoruese vendase dhe ndërkombëtare në lidhje me garantimin e dhënies së drejtësisë sipas standardeve të përcaktuara në ligj, studimet shkencore për aspekte të tjera të përdorimit të teknologjisë janë të pakta.

3. Standardet ndërkombëtare për mbrojtjen e viktimave dhe përdorimi i teknologjisë

Rreth tre dekada më parë, viktimat nuk mund të dëgjoheshin direkt për shqetësimet e tyre në shumë juridiksione.[16] Nga miratimi i Deklaratës së

14 Udhëzimi nr.8, datë 15.11.2021 të Prokurorit Përgjithshëm "Hetimi dhe ndjekja penale efektive të veprave penale me të mitur në konflikt me ligjin, fëmijët viktima dhe/ose dëshmitar". Dokumenti u aksesua në datën 18 Qershor 2022.

15 Ligji nr.95/2016 "Për organizimin dhe funksionin e institucioneve për të luftuar korrupsionin dhe krimin e organizuar", neni 25.

16 Shih: Guide for policy makers on the implementation of Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, botim i CICP, 1999, fq.20. Dokumenti gjendet në adresën: https://www.unodc.org/pdf/criminal_justice/UNODC_Guide_for_Policy_Makers_Victims_of_Crime_and_Abuse_of_Power.pdf. Dokumenti u aksesua në 18 Qershor 2022.

Kombeve të Bashkuara për Parimet Themelore të Drejtësisë në lidhje me Viktimat e Kriminalitetit dhe Abuzimit të Pushtetit (1985), trajtimi i viktimës në sistemin e drejtësisë penale ka evoluar. Deklarata i kërkon shteteve të marrin masa për të kufizuar sa më shumë vështirësitë që hasin viktimat, për t'i mbrojtur jetën private dhe garantuar sigurinë e tyre dhe të familjes nga manovrat dhe raprezaljet (paragrafi 5, gërma "ç"). Deklarata i mundëson viktimës për tu dëgjuar dhe të paraqitur vet shqetësimet e saja. Udhëzuesi i Deklaratës (1999) përmban modele pozitive sesi mund të mbrohet viktima, sidomos i mituri viktimë dhe viktima e dhunës seksuale duke sugjeruar sigurimin e dëshmisë së filmuar ose përdorimin e pasqyrave njëkahëshe aty ku kjo do të inkurajë viktimën të flasë më lirshëm, si në rastin e viktimave të sulmit seksual ose fëmijët viktima[17].

Nga miratimi i deklaratës, një sërë aktete ndërkombëtare parashikojnë mbrojtjen e dëshmitarëve dhe viktimave përmes përdorimit të teknologjisë së komunikimit ose mjeteve të tjera. Konventa kundër krimit të organizuar transnacional,[18] Protokolli "Për parandalimin, shtypjen dhe ndëshkimin e trafikimit të njerëzve, veçanërisht grave dhe fëmijëve",[19] Konventa e Kombeve të Bashkuara kundër korrupsionit (neni 32&2); Konventa e Këshillit të Europës për parandalimin dhe luftimin e dhunës kundër grave dhe dhunës në familje (Konventa e Stambollit);[20] Konventa e Këshillit të Evropës për mbrojtjen e fëmijëve nga shfrytëzimi seksual dhe abuzimi seksual (Konventa e Lazorones) [21] etj. parashikojnë përdorimin e teknologjisë të nevojshme të komunikimit në pyetjen e viktimës dhe dëshmitarit. Teknologjia përdoret për regjistrimin dhe ruajtjen e të dhënave të personave, si gjurmët e gishtave, identiteti dhe profili gjenetik (ADN). Për shembull, Konventa e Lazarones parashikon regjistrimin dhe ruajtjen e të dhënave kombëtare për të dënuarit për vepra seksuale. Përdorimi i teknologjisë dhe mbrojtja e të dhënave

17 Po aty, fq.22.

18 Ligj nr. 8920 datë 11.7.2002 Për ratifikimin e "Konventës së Kombeve të Bashkuara kundër krimit të organizuar ndërkombëtar" dhe dy protokolleve shtesë të saj, nenet 24-26.

19 Protokolli "Mbi parandalimin, pengimin dhe ndëshkimin e trafikut të personave, veçanërisht të grave dhe fëmijëve, në plotësim të Konventës së Kombeve të Bashkuara kundër krimit të organizuar ndërkombëtar, nenet 6-8.

20 Konventa e Këshillit të Europës për parandalimin dhe luftimin e dhunës kundër grave dhe dhunës në familje, neni neni 56, shkronja "f", "g", "i". Konventa u aksesua në adresën: https://rm.coe.int/168046246b.

21 Konventa e Këshillit të Evropës për Mbrojtjen e Fëmijëve nga Shfrytëzimi Seksual dhe Abuzimi Seksual, neni 35&2. Konventa u aksesua në adresën: https://rm.coe.int/168046e1e3.

personale që është një sfidë e madhe me të cilën përballet shoqëria e sotme nuk është pjesë e kësaj kumtese.

4. Teknologjia, viktimat dhe drejtësia penale për të mitur në Shqipëri

Drejtësia për viktimën, përfshirë fëmijën viktimë ishte pak e njohur dhe zbatuar në drejtësinë penale shqiptare. Deri pak vite më parë, viktima dëgjohej në procesin penal si dëshmitare. Pas ndryshimeve të miratuara në Kodin e Procedurës Penale (KPP) në vitin 201722 të drejtat e viktimës së veprës penale u parashikuan më mirë në ligj. Sipas ligjit viktima ka të drejtë, ndër të tjera, të thirret në seancën paraprake dhe në seancën e parë gjyqësore; të dëgjohet nga gjykata, edhe kur asnjëra nga palët nuk ka kërkuar thirrjen e saj si dëshmitar.23 Të drejta shtesë parashikohen për fëmijën viktimë (neni 58/a i KPP), viktimat e dhunës seksuale dhe të trafikimit (neni 58/b i KPP).

Trajtimi i fëmijës viktimë rregullohet në mënyrë të detajuar nga kodi i drejtësisë penale për të miturit (KDPM), kodi penal (KP) dhe KPP. Mbrojtja e të drejtave të fëmijës dëshmitar dhe/ose viktimë e veprës penale, parandalimi i riviktimizimin dhe viktimizimin e dytë të fëmijës janë dy nga qëllimet e kodit të drejtësisë penale për të mitur (paragrafi 4 dhe 5 i nenit 2 të KDPM).[24]

Ligji detyron profesionistët që punojnë me dhe për fëmijët vlerësimin me përparësi të interesit më të lartë të fëmijës, ndër të cilat nevojat e tij për siguri, historinë e fëmijës si: situatat e veçanta të abuzimit, neglizhencës, shfrytëzimit, ose forma të tjera të dhunës si dhe rrezikun që situata të ngjashme të ndodhin në të ardhmen në çdo veprim të policisë, prokurorisë ose gjykatës.[25] Nevoja për një mjedis të sigurt dhe siguria e viktimës nga traumatizimi i mëtejshëm mund të vërë në diskutim përballjen e viktimës dhe pyetjen e saj me praninë fizike të autorit të krimit. Pjesëmarrja në proces duke zbatuar teknologjinë në pyetjen e tij është një nga masat për mbrojtjen e viktimës, përfshirë viktimën e mitur.[26] Megjithatë, në realizimin e të drejtës për tu dëgjuar, nëse është në interesin më të lartë të viktimës, prokurori dhe gjykata kanë detyrimin të krijojnë të gjitha kushtet dhe të marrin çdo masë

22 Ligji nr. 35/2017, datë 30.3.2017.

23 Neni 58, shkronjat "h", "i" të Kodit të Precedurës Penale.

24 Riviktimizimi dhe viktimizimi i dytë janë situata të përkufizuara dhe të adresuara në KDPM.

25 Neni 10 i KDPM.

26 Neni 16 i Kodit të Drejtësisë Penale për të Mitur.

për të nxitur pjesëmarrjen e viktimës në procedimin penal, por jo kur viktima është fëmijë.

Një nga çështjet që me interes për tu trajtuar është se kur duhet të përdoret teknologjia dhe kush vendos për përdorimin e saj për të garantuar siguri për viktimën në procesin penal. KDPM nuk parashikon përdorimin e detyruar të teknologjisë në çdo rast që ka një viktimë. Për më tepër, viktima mund të jenë në rrezik para, pas denoncimit të ngjarjes, para fillimit, gjatë zhvillimit ose përfundimit të procesit penal. Siguria dhe mbrojtja e viktimës nevojiten të adresohen në çdo fazë, duke parashikuar marrjen e masave për raportimin e rrezikut.[27] Sikurse u theksua më lart, një nga masat mbrojtëse është shmangia e kontakteve të viktimës me autorin, gjatë pyetjes, ballafaqimit, zhvillimi i seancës mes përdorimit të mjeteve të teknologjisë.

Përcaktimi i nevojës dhe momentit të përdorimit të teknologjisë dhe balanca me garantimin e së drejtës e të akuzuarit për t'u dëgjuar, ballafaquar me viktimën, e drejta për një proces të rregullt nuk janë gjithnjë çështje të lehta në praktikë. Vështirësitë janë të karakterit objektiv dhe subjektiv si: mungesa e teknologjisë së nevojshme dhe mjediseve miqësore për viktimën, sidomos fëmijët viktimë, diskrecioni i dhënë prokurorit dhe gjyqtarit për të vlerësuar nevojën e përdorimit të teknologjisë dhe kuptimi dhe zbatimi jo i njëjtë i ligjit nga profesionistët, nevoja e balacimit mes sigurisë së viktimës dhe të drejtës së të akuzuarit dhe përfaqësuesit ligjor të tij të bëjë pyetje ose kundërshtime të dëshmisë së viktimës, garantimi i procesit të rregull ligjor etj. ndikojnë në vendimmarrjen për përdorimin e teknologjisë për intervistimin e viktimës dhe shmangien e ballafaqimit të saj me autorin e krimit.

Mënyra e formulimit të nenit 58/a të KPP lë të kuptohet se regjistrimi me mjete audiovizive jo gjithnjë është i detyrueshëm dhe se vendimi për përdorimin e tyre merret kur përmbushen dy kritere: përdorimi i teknologjisë të jetë "i përshtatshëm" dhe "e mundur". Pra, dy kriteret e parashikuara nga ligji janë kumulative. Në praktikë mund të ndodhë që përdorimi i teknologjisë është i përshtatshëm, por jo i mundur, ose e anasjellta.

Kuptimi i termit "i përshtatshëm" detajohet në KDPM, në rastin e viktimës së mitur. Qëllimi është mospërkeqësimi i traumë së përjetuar nga mituri viktimë dhe nga ana tjetër, sistemi i drejtësisë t'i sigurojë fëmijës ndihmën e duhur, sipas rastit dhe nevojave të tij (nenin 17 i KDPM). Ligji parashikon

27 Guidelines on justice in matters involving child victims and witnesses of crime. https://www.un.org/ruleoflaw/files/UNGuidelinesChildVictimsWitnesses.pdf. Dokumenti u aksesua në datë 16 Qershor 2022.

një sërë masash mbrojtëse që marrin sipas rastit, prokurori, policia gjyqësore ose Njësia për Mbrojtjen e të Drejtave të Fëmijës në rast se i mituri është në rrezik mes të cilave shmangia e kontaktit të drejtpërdrejtë midis të miturit viktimë ose dëshmitar dhe të akuzuarit, në çdo fazë të procesit. [28]

Shmangia e kontaktit të drejtëpërdrejtë midis viktimës dhe të akuzuarit, viktimës fëmijë dhe të akuzurit bën të përshtatshme përdorimin e teknologjisë, por nuk nënkupton se i mituri nuk do të dëgjohet dhe marrë pjesë në proces. KDPM (neni 39-43) parashikon rregulla të veçanta të pyetjes së të miturit viktimë ose dëshmitar. Sipas nenin 39 të KDPM kur dhënia e dëshmisë e vendos të miturin në rrezik serioz për jetën dhe shëndetin, mund të përdoret të ndryshme për ët cilat vjen në ndihmë teknologjia. *Së pari*, gjyqtari garanton pyetjen e dëshmitarit/viktimë të mitur duke përdorur pajisje që ndryshojnë pamjen dhe/ose zërin e dëshmitarit/viktimës. S*ë dyti*, marrja në pyetje e të miturit viktimë pas një ekrani jotransparent ose marrjen në pyetje në distancë. Së treti, pyetja e dëshmitarit/viktimë të mitur përpara fillimit të seancës gjyqësore me pjesëmarrjen e mbrojtësit të të miturit dhe videoregjistrimit të pyetjes së të miturit.

Përdorimi i teknologjisë në pyetjen e të miturit viktimë shoqërohet me garanci të tjera që mbrojnë fëmijën. Për viktimën fëmijë, biseda regjistrohet me mjete audiovizive kur është e mundur dhe e përshtatshme, regjistrimi mund të përdoret si provë në procedimin penal dhe vlerësohet, pyetja pa vonesë nga persona të specializuar, shqyrtimi pa vonesë dhe me përparësi i çështjeve me të mitur viktimë dhe dëshmitar pa cënuar garancitë e procesit penal si dhe pjesëmarrja e detyrueshme e psikologut[29] gjatë pyetjes së të miturit viktimë ose dëshmitar janë garanci për sigurinë e viktimës.

Në rastin e një fëmijë viktimë, pyetja shtrohet kush përcakton faktin se fëmijës i kanoset një rrezik dhe lloji i tij? Standardet kërkojnë që ky vlerësim të bëhet nga organet përkatëse, mes vlerësimit të riskut, ndërsa masat mbrojtëse mund të merren nga policia, prokuroria dhe gjykata, me ndihmën e psikologut. Shprehja që përdoret në ligj se “kur dhënia e dëshmisë mund ta vendosë viktimën e mitur në rrezik për jetën ose shëndetin”, gjyqtari garanton pyetjen e fëmijës viktimë duke përdorur teknika të posacme të përcaktuara në ligj” vë në pah nevojën, jo vetëm të paisjes me teknologji të policisë, seksioneve për të miturit në gjykata dhe prokurori, por nevojën e trajnimit të personelit me teknikat e intervistimit dhe aftësimin për vlerësimin e rrezikut

28 Kodi i Drejtësisë Penale për të Mitur, neni 37, paragrafi 1, shkronjat “a”.

29 Neni 17 i Kodit të Drejtësisë Penale për të Mitur.

të fëmijës.[30]

Referuar praktikës shqiptare, mjedise miqësore janë krijuar në një pjesë të komisariateve të policisë dhe ato janë të paisura me mjetet e intervistimit[31]. Harta e re gjyqësore dikton nevojën e vlerësimit të mjediseve miqësore dhe krijimit të tyre aty ku ato mungojnë. Gjithashtu, mjediset e krijuara, mjetet e intervistimit dhe regjistrimit audio vidio të dëshmisë nga policia që në momentin e parë duhet shfrytëzuar në çdo rast që fëmija është në kontakt/ konflikt me ligjin. Kjo kërkon një rritje të profesionalizmit të punonjësve të policisë në metodat e intervistimit dhe marrjen e dëshmisë duke respektuar parashikimet ligjore në lidhje me garantimin e procesit të rregullt ligjor dhe realizimin e të drejtave të të akuzuarit.

Teknologjia është e nevojshme dhe përdorimi i saj është i detyrueshëm në rastin e pyetjes së të miturit viktimë dhe/ose dëshmitar të shfrytëzimit seksuale ose dhunës seksuale, regjistrimi audio. Dëshmia në audio dhe video e dhënë nga i mituri mund të shfaqet gjatë seancës gjyqësore[32] dhe ajo mund të dëgjohet në sallën e gjyqit pa qenë i pranishëm vetë i mituri, nëpërmjet përdorimit të teknologjive të nevojshme të komunikimit. Në një rast të tillë, teknologjia, jo vetëm mundëson mbrojtje dhe siguri për fëmijën viktimë, shmanget riviktimizimi i fëmijës duke e pyetur atë mundësisht një herë, shmanget përballja me të pandehurin, etj, por procesi është efektiv për fëmijën. Gjithashtu, sigurimi menjëherë i provës dhe pyetja vetëm një herë i fëmijës, përdorimi i regjistrimit të pyetjes në fazat e tjera të procedimit kërkon respektimit e garancive të tjera që dëshmia të mos kundërshtohet në fazat e tjera, veçanërisht garantimi i së drejtave të të akuzuarit për tu njoftuar për pyetjen, për të bërë drejtëpërdrejtë ose indirekt pyetje viktimës, për të kundërshtuar pjesë të dëshmisë etj..

30 Një pjesë e mjediseve të policisë janë rikonstruktuar sipas standardeve më të mira dhe miqësore për fëmijët dhe janë paisur me teknologjinë e intervistimit. Harta e re gjyqësore dikton nevojën e vlerësimit të mjediseve miqësore dhe krijimit të tyre aty ku ato mungojnë ose përdorimin gjithnjë e më të gjerë të regjistrimit audio dhe vidio të dëshmisë së dhënë në polici. Kjo kërkon një rritje të profesionalizmit të profesionistëve në metodat e intervistimit dhe marrjen e dëshmisë duke respektuar parashikimet ligjore.

31 Strategjia e Drejtësisë për të Mitur, Raport monitorimi, Janar- Dhjetor 2021, botim i Ministrisë së Drejtësisë, 2021, fq.71-72. Shih: https://www.drejtesia.gov.al/wp-content/uploads/2022/04/Raporti-i-Monitorimit-t%C3%AB-Strategjis%C3%AB-s%C3%AB-Drejt%C3%ABsis%C3%AB-p%C3%ABr-t%C3%AB-Mitur-p%C3%ABr-periudh%C3%ABn-janar-dhjetor-2021.pdf. Dokumenti i aksesua më datë 8 Gusht 2022.

32 Neni 58/b i Kodit të Procedurës Penale.

Sa më sipër, përdorimi i teknologjisë në pyetjen e viktimës në një mjedis miqësor për të, e zbatuar nga profesionistë krahas mundësisë së zhvillimit të proceseve me dyer të mbyllura dhe respektimi i të drejtavetë të akuzuarit janë garanci procedurale që mundësojmë mbrojtjen e viktimës dhe të interesit të saj.

Teknologjia përdoret edhe për pyetjen e dëshmitarëve, përfshirë pyetjen në distancë të tyre Neni 361, paragrafi 7 dhe 8 i KPP parashikon se dëshmitari mund të pyetet në distancë, brenda ose jashtë vendit, me anë të lidhjes audiovizive. Përdorimi i teknologjisë shoqërohet me respektimin e disa garancive për të të pasur një proces penal të rregullt si personi i autorizuar nga gjykata qëndron në vendin ku ndodhet dëshmitari dhe bën vërtetimin e identitetit të tij; kujdeset për zhvillimin e rregullt të marrjes në pyetje e për zbatimin e masave të mbrojtjes. Veprimet e kryera pasqyron në procesverbal.

Ligji parashikon garanci procedurale për pyetjen e dëshmiratit të mitur nën moshën 14 vjeç dhe atij të moshës 14-18 vjeç. Sipas nenit 361/a të KPP, pyetja e dëshmitarit të mitur nën moshën 14 vjeç[33] bëhet pa praninë e gjyqtarit, pyetja bëhet nëpërmjet një psikologu, edukatori ose ndonjë eksperti tjetër në një mjedis miqësor për fëmijë, kur është e mundur nëpërmjet mjeteve audiovizive. Prindërit ose kujdestari mund të jenë të pranishëm gjatë marrjes në pyetje dhe kur nuk është në kundërshtim me interesat e gjykimit ose të fëmijës. Ligji parashikon mundësinë që kur palët e kërkojnë i mituri të merret në pyetje nga gjyqtari në prani të ekspertit. Në këtë rast gjykata merr vendimin përkatës. I mituri merret në pyetje sërish vetëm në raste të veçanta dhe sipas të njëjtës procedurë. Pyetja e dëshmitarit të mitur 14 deri në 18 vjeç kryhet nga kryetari i trupit gjykues. Kur dëshmitari është viktimë, ai mund të pyetet nga një psikolog në një mjedis miqësor për të dhe kur është e mundur duke përdorur mjetet audiovizive.

Një nga përparësitë e regjistrimit të dëshmisë së fëmijës është mundësia e pyetjes vetëm njeherë dhe shmangia e ripyetjes të tij që mund të shkaktojë stres dhe trauma të reja, të thellojë traumën e pësuar nga fëmija. Çdo palë mund t'i referohet pyetjes dhe fëmija nuk ndryshon dhënien në gjykata ose sa herë që pyetet. Ligji përcakton se kur i mituri është dëgjuar gjatë hetimit dhe deklarimet e tij janë regjistruar, ato përdoren si provë në gjykim nëse i pandehuri dhe mbrojtësi japin pëlqimin. Deklarimet e të miturit mund të përdoren si provë edhe nëse mbrojtësi është lejuar të pyesë të miturin

33 Shtuar me ligjin nr. 9276, datë 16.9.2004 dhe ndryshuar neni me ligjin nr. 35/2017, datë 30.3.2017.

nëpërmjet profesionistëve dhe eksperti shpreh mendim se përsëritja e pyetjes mund të dëmtojë kushtet psikologjike të të miturit.[34]

Nëse i referohemi praktikës gjyqësore, nga kërkimet e kryera nuk u gjend ndonjë studim në lidhje me përdorimin i teknologjisë për mbrojtjen e fëmijëve viktimë, por ka të dhëna të shpërndara në raporte monitorimi ose vlerësimi të projekteve që zbatohen për drejtësinë e të miturve. Pas pesë viteve të zbatimit të Kodit të Drejtësisë Penale për të Mitur dhe miratimti të ndryshimeve në KPP do të ishte me interes kryeja e studimi vlerësues në lidhje me përdorimin e teknologjisë dhe ndikimin e saj në mbrojtjen e fëmijës viktimë nga riviktimizimi.

5. Përdorimi i teknologjisë, procesi i rregullt ligjor dhe moscënimi i jetës private

Përdorimi teknologjisë në proceset penale adreson çështje që kanë të bëjnë me respektimin e të drejtave të palëve në proces, garantimi i të drejtave të viktimës dhe të pandehurit në procedimet penale. Respektim i procesit të rregullt ligjor gjatë gjithë fazave, mbrojtja dhe siguria e viktimës, shpesh është vënë në diskutim dhe ka qënë objekt shqyrtimi në Gjykatën Evropiane për të Drejtat e Njeriut (GJEDNJ).

Sipas një raporti të BE-së, studimet kanë vënë në pah se përdorimi i teknologjisë në komunikimet mes avokatëve dhe klientëve të tyre mund të riskojë komunikimin konfidencial gjatë seancave në distancë. Gjatë procedurave të mbajtura nëpërmjet videokonferencës disa kategori personash që kanë nevoja të veçanta si aftësi të kufizuar dëgjimi, ose të kuptuarit të ligjit mund të cënohen në ushtrimin e së drejtës së tyre për një gjykim të drejtë, për pjesëmarrje efektive në gjyqësor si dhe mund të diskriminohen.[35]

Më shumë se një herë GJEDNJ ka theksuar se përdorimi i regjistrimit të pyetjes së viktimës me sistemit audio vidio nuk cënon të drejtat e të pandehurit dhe parimet e procesit të rregullt ligjor, nëse të pandehurit i garantohet e drejta të njoftohet për dëshminë, njihet me dëshminë, të adresojmë pyetje për viktimën, dhe të ketë të drejtë të kundërshtojë pjesë të deklarime të regjistruara. Gjithashtu, fëmija mund të ripyetet kur pjesë të regjistrimit kundërshtohen nga i akuzuari, por duke respektuar garancitë ligjore si largimi nga seanca e të akuzuari, përdorimi i mjeteve që shmangin

34 Neni 58/a, paragrafi 4 i Kodit të Procedurës Penale.

35 Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age, Sergio Carrera Valsamis Mitsilegas Marco Stefan, vep. e cit, fq. 38-39.

shikimin mes tyre etj.

Gjykata e Evropianë e të drejtave të njeriut në një nga vendimet e saj ka theksuar se:

44. Gjykata duhet të ketë parasysh edhe veçoritë e procedurave penale në lidhje me krimet seksuale. Procedura të tilla shpesh përbëjnë një një sprovë për viktimën, veçanërisht kur kjo e fundit nuk ka dëshirë të ballafaqohet me të pandehurin. Këto veçori janë edhe më të theksuara në rastin që përfshin një të mitur. Në vlerësimin e pyetjes nëse i akuzuari ka pasur ose jo një gjykim të drejtë në këto procedura, duhet pasur parasysh respektimin e së drejtës për jetës private të viktimës së supozuar. Gjykata pranon se në procedurën penale lidhur me abuzimin seksual mund të merren masa të caktuara për mbrojtjen e viktimës, me kusht që masat e tilla të mund të harmonizohen me një adekuate dhe ushtrimi efektiv i të drejtave të mbrojtjes (shih, për shembull, Aigner, cituar më sipër, § 35; A.S. kundër Finlandës, cituar më sipër, § 55; S.N. kundër Suedisë, cituar më sipër, § 47; dhe Vronchenko, cituar më lart, § 56).

45. Duke pranuar nevojën për të vendosur një ekuilibër ndërmjet të drejtave të të pandehurit dhe atyre të fëmijës viktimë, Gjykata ka konstatuar se duhet të ekzistojnë garancitë minimale të mëposhtme: personi i dyshuar duhet të informohet për dëgjimin e fëmijës, atij ose asaj duhet t'i jepet një mundësia për të vëzhguar atë seancë, qoftë kur po zhvillohet ose më vonë nga një regjistrim audiovizual dhe për t'i bërë pyetje fëmijës drejtpërdrejt ose tërthorazi, gjatë seancës së parë ose në një rast të mëvonshëm (shih A.S. kundër Finlandës, cituar më lart, § 56).[36]

GJEDNJ në vendimin W.S. kundër Polonisë, datë 17.06.2007, ka arsyetuar se:

59. Ndryshe nga shumë raste të tjera në të cilat Gjykata shqyrtoi ankesa të ngjashme, provat vendimtare për të cilat kërkuesi u dënua mund të kundërshtoheshin para gjykatës (shih në këtë aspekt, mutatis mutandis, Van Mechelen dhe të tjerët kundër Hollandës, cituar më lart, §§ 51-55, shih gjithashtu Kostovski kundër Holandës, aktgjykimi i 20 nëntorit 1989, Seria A nr. 166, f. 20, § 41). Megjithatë, për Gjykatën, dhe si çështje drejtësie, duhet të ishin marrë masat e duhura për t'i lejuar gjykatës që të merrte një pamje më të gjerë të çështjes së fajit të mundshëm të kërkuesit. Ai vëren se në asnjë fazë nuk është marrë parasysh mundësia e regjistrimit me video të

36 Vendimi i GJEDNJ Eduardo González Nájera kundër Spanjës, aplikimi nr. 61047/13. Vendimi është i aksesueshën në adresën: http://hudoc.echr.coe.int/webservices/content/pdf/001-141859?TID=ihgdqbxnfi. Dokumenti u aksesua në datën 8 Gusht 2022.

seancave të cilat E.K. kishte pasur me X. Është për t'u vërejtur në lidhje me këtë se ankesa është bërë në prokurori më 14 prill 1994 dhe se E.K. ishte në gjendje të kryente një intervistë të parë me fëmijën në të njëjtën datë. Një intervistë tjetër u zhvillua më 9 janar 1995. Në asnjë rast nuk u bë një video-incizim që tregonte se si E.K. kishte ndërvepruar me fëmijën dhe ishte përpjekur të krijonte një opinion nëse akuzat për abuzim seksual ishin të bazuara dhe nëse aplikanti ishte i implikuar.[37]

Përdorimi i teknologjisë në mbrojtje të viktimave të krimeve seksuale është cituar nga gjykata edhe në paragrafin 61 të po këtij vendimi ku gjykata ndër të tjera nënvizon rëndësinë e regjistrimit të intervistës së viktimës kur nuk është e mundur marrja në pyetje e saj ose ballafaqimi me të pandehurin duke e konsideruar cënim të procesit të rregullt ligjor, shkelje të nenit 6 të konventës:

" Në çështjen në fjalë, thelbi i kërkesës së aplikuesit është që viktima e veprës penale nuk është marrë asnjëherë në pyetje gjatë proçesit dhe, si rezultat i kësaj, ajo është dënuar pa i'u dhënë mundësia të merrej në pyetje. ..... Nëse në këtë çështje autoritetet do të kishin marrë masa të cilat do të lejonin gjykatën të kishtë në dispozicionin e saj, për shëmbull, një regjistrim të intervistës së psikologut me viktimën, mbrojtja e aplikuesit do të ishte e orientuar më mirë."[38]

E drejta e të miturit për jetë private duhet të respektohet plotësisht në çdo fazë të drejtësisë penale për të mitur duke bërë kujdes që të shmanget dëmtimi i tij. Kjo nënkuptin se nuk publikohet asnjë informacion që mund të çojë në identifikimin e të miturit viktimë ose dëshmitar i një vepre penale. Kodi i Drejtësisë Penale për të Mitur[39] parashikon masa që mund të merren për të mbrojtur jetën private dhe mirëqenien e të miturve viktima dhe dëshmitarë si: mosidentifikimi i të miturit, duke ndryshuar imazhin/pamjen/ figurën ose të zërin; vendosjen e një mburoje jo të tejdukshme; pyetjen në një mjedis tjetër dhe transmetimin në të njëjtën kohë në sallën e gjykimit me anë të televizionit me qark të mbyllur; filmimin (regjistrimit me zë dhe me figurë) të pyetjes së dëshmitarit të mitur përpara seancës, rast në të cilin mbrojtësi i të akuzuarit merr pjesë në shqyrtim dhe i jepet mundësia t'i bëjë pyetje të miturit dëshmitar ose viktimë.

37 Vendimi i GJEDNJ W.S. *kundër* Polonisë, 24.09.2007. Aplikimi nr. 21508/02. Vendimi u aksesua në adresën: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-81140%22]}. Dokumenti u aksesua në datën 18 Qershor 2022.

38 Po aty.

39 Neni 43 i Kodit të Drejtësisë Penale për të Mitur.

GJEDNJ në një vendim të saj që ka të bëjë me një abuzim seksual ka vënë theksin në rëndësinë e mbrojtjes së jetës private të viktimës dhe në detyrimin e shtetit që të parandalojnë riviktimizimin e viktimës në çdo fazë të procesit, duke zhvilluar seancat më dyer të mbyllura, pavarësisht se viktima kishte dhënë intervistë në media. Gjykata e gjeti të rëndësishme të theksonte se "*detajet intime nga jeta e një viktime të dhunës seksuale mund të zbulohet në çdo fazë të gjykimit penal kundër autorit të supozuar dhe jo vetëm gjatë marrjes në pyetje të tërthortë të viktimës. Rrjedhimisht, zhvillimi i mbyllur vetëm e një pjese të procedurave nuk do të mjaftonin për të mbrojtur të drejtat e viktimës, në veçanti në çështje që kishin të bënin me nevojën për të mbrojtur integritetin dhe dinjitetin e viktimës, dhe për mbrojtjen e saj nga sikleti dhe stigmatizimi i mëtejshëm".* [40]

Një një vendim tjetër, GJEDNJ vë në pah një procedim jo e efektiv të fëmijës viktimë duke konstatuar shkelje të nenit 3 dhe 8 të KEDNJ. Në vendimin e saj Gjykata u shpreh *se " kishte pasur shkelje të nenit 3 (ndalimi i çnjerëzor ose trajtim degradues) dhe 8 (e drejta për respektimin e jetës private dhe familjare) të Konventës, duke konstatuar se sjellja e autoriteteve kombëtare nuk ishte në përputhje me detyrimin për të mbrojtur një fëmijë që kishte qenë viktimë e shfrytëzimit dhe abuzimit seksual. Ajo konstatoi veçanërisht se mungesa e mbështetjes për kërkuesin, mosmbrojtja e saj kundër të pandehurve, rindërtimi i panevojshëm i incidenteve të përdhunimit, ekzaminimet e përsëritura mjekësore, mungesa e një ambienti të qetë dhe të sigurt në seancat, vlerësimi i pëlqimit të viktimës, zgjatja e tepërt e procedimet dhe, së fundi, fakti që dy nga akuzat ishin parashkruar, përbën një rast të rëndë të viktimizimit dytësor të kërkuesit. Në vlerësimin e Gjykatës, mënyra sesi procedimi ishte zhvilluar nuk kishte siguruar zbatimi efektiv të ligjit penal dhe ka cenuar vlerat e mbrojtura nga nenet 3 dhe 8 të Konventës.*[41]

Pavarësisht, parashikimeve ligjore, identifikimi i fëmijës në kontakt ose konflikt me ligjin në proceset penale shqiptare bëhet në forma të ndryshme si me praninë fizike të tij gjatë procedimit penal dhe seancën gjyqësore ose mes publikimit në çfarëdolloj forme i të dhënave personale të fëmijës, kur nuk respektohet kushtet dhe kriteret e parashikuara në legjislacionin

40 Çështja Mraović *kundër* Kroacisë, aplikimi nr. 30373/13. Përmbledhja e vendimit është e aksesueshme në adreswn: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12787%22]}. Dokumenti u aksesua më datë 25.09.2022.

41 Vendimi i GJEDNJ N.Ç. *kundër* Turqisë, aplikimi nr. 40591/1. Vendimi u aksesua në adresën: https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6931183-9316853%22]}. Dokumenti u aksesua më datë 25.09.2022.

për mbrojtjen e të dhënave personale. Megjithëse Kodi i Transmetimit për mediat audiovizive[42] parashikon rregulla që nuk lejojnë identifikimin direkt ose indirekt të fëmijës, në kontakt/ konflikt me ligjin, ky i fundit është i ekspozuar në media, të dhënat personale të tij publikohen, veçanërisht nga mediat online.

Sa më sipër, përdorimi i teknologjisë në proceset penale nuk mjafton nëse ajo nuk shoqërohet me garanci të tjera ligjore që parandalojnë cënimin e jetës private, të dhënave personale dhe dinjitetin e viktimës gjatë gjithë fazave të procesit.

Përfundime dhe rekomandine

Teknologjia dhe zhvillimet e saj përdoren në sistemin e drejtësisë penale për një menaxhim më efektiv të tij, dhe për të mundësuar siguri, mbrojtje të viktimave dhe dëshmitarëve. Përdorimi i teknologjisë ngre një sërë çështjesh që kanë të bëjnë me barazinë e palëve në proces, procesin e rregullt ligjor dhe respektimin e të drejtave të njeriut. Jurisprudenca e GJEDNJ në lidhje me përdorimin e teknologjisë në sistemin e drejtësisë penale pasurohet. Njohja e praktikës së GJEDNJ dhe zbatimi i saj do të ndihmojnë në balancimin e interesave të palëve dhe mbrojtjen e të drejtave të njeriut në drejtësinë penale.

Referuar Shqipërisë, përdorimi i teknologjisë për mbrojtjen e fëmijës në kontakt/konflikt me ligjin është parashikuar nga legjislacioni shqiptar. Përdorimi i saj në kushtet ne përcaktura në ligj është detyrim që buron nga konventat ku shteti shqiptar është palë dhe nga legjislacioni shqiptar në fuqi. Njohja, kuptimi dhe zbatimi i drejtë i ligjit nga të gjithë profesionistët në lidhje me kushtet se kur dhe si përdoret teknologjia është me rëndësi.

Na ana tjetër, mundësitë e përdorimit të teknologjisë janë të ndërvarura nga disa faktorë. *Së pari*, mjediset e intervistimit duhet të jenë të paisura me mjetet e teknologjisë së avancuar audio vidio. *Së dyti*, ekzistenca e mjediseve miqësore në polici, prokurori dhe gjykatë për fëmijën viktimë. *Së treti*, përdorimi i mjediseve miqësore dhe i paisjeve teknologjike aty ku ekzistojnë. *Së katërti*, niveli i trajnimit të profesionistëve për të vlerësuar riskun dhe faktorët e riskut me qëllim parandalimin e rrezikut ose dëmtimet

42 Kodi i Transmetimit për Median Audiovizive, miratuar me Vendimin e AMA-s, nr. 228, datë 11.12.2017. Shih: http://ama.gov.al/wp-content/uploads/2018/05/Kodi-i-Transmetimit-p%C3%ABr-Median-Audiovizive.pdf. Dokumenti u aksesua në datën 15. 09.2022.

ndaj viktimës së mitur dhe/ose dëshmitarë. *Së pesti*, fuqizimi i kapaciteteve të punonjësve që mirëmbajnë dhe përdorin teknologjinë.

Në promovimin e përdorimit të teknologjisë, balanca mes nevojës së sigurisë së viktimës, dëshmitarit dhe garantimit të barazisë së palëve, procesit të rregullt ligjor duhet të mbahen parasysh dhe të respektohet. Praktikat e mira në lidhje me përdorimin e teknologjisë sistemin e drejtësisë penale dhe ndikimin e tyre në garantimin e të drejtave të palëve për një proces të rregullt ligjor duhen promovuar dhe njohur nga profesionsitët e praktikës.

Studimet shkencore që vlerësojnë shkallën e përdorimit të teknologjisë në proceset penale ku fëmija është në kontakt/konflikt me ligjin dhe ndikimi që ajo ka sjelljë për viktimën në procesin penal, trajtimi i aspekteve të balacës mes përdorimit të tekonlogjisë dhe procesit të rregult ligjor janë të nevojshme.

Së fundi, digjitalizimi i sistemit të drejtësisë penale dhe përdorimi i teknologjisë në proceset penale kërkon mbështetje me burime njerëzore dhe financiare,tekonologji të avancuar, kujdes për mirëmbajtjen e sistemeve dhe mbrojtjen e të dhënave të tyre nga dëmtimet, sulmet kibernetike dhe keqpërdorimi i tyre.

Literatura

Donna M. Hughes: Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies, botuar në SAGE OpenVolume 4, Issue 4, October-December 2014. Shih: https://journals.sagepub.com/doi/epub/10.1177/2158244014553585

Florian Bonensteffen, Sven zebel & Ellen Giebels: Is computer-based communication a valuable addition to victim-offender mediation? A qualitative exploration among victims, offenders and mediators, victims & offenders, (2022):. Shih: doi: 10.1080/15564886.2021.2020946, https://doi.org/10.1080/15564886.2021.2020946. Dokumenti është aksesuar me datë 8 Gusht 2022.

Sergio Carrera, Valsamis Mitsilegas, Marco Stefan: Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age, botim i Centre for European Policy Studies (CEPS), Bruksel, Maj 2021. Shih: https://ëëë.ceps.eu/ëp-content/uploads/2021/05/Criminal-Justice-Fundamental-Rights-and-the-Rule-of-laë-in-the-Digital-Age.pdf

Akte ndërkombëtare, strategji dhe dokumente politikash

Guide for policy makers on the implementation of Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, botim i CICP, 1999, fq.20. Dokumenti gjendet në adresën: https://www.unodc.org/pdf/criminal_justice/UNODC_Guide_for_

Policy_Makers_Victims_of_Crime_and_Abuse_of_Power.pdf.

Guidelines on justice in matters involving child victims and witnesses of crime. https://www.un.org/ruleoflaë/files/UNGuidelinesChildVictimsWitnesses.pdf

Guidelines on videoconferencing in judicial proceedings, CEPEJ, Këshilli i Evropës, 2021. Shih:

https://rm.coe.int/cepej-2021-4-guidelines-videoconference-en/1680a2c2f4

Konventa e Këshillit të Evropës për mbrojtjen e fëmijëve nga shfrytëzimi seksual dhe abuzimi seksual. https://rm.coe.int/168046e1e3

Konventa e Këshillit të Evuropës për parandalimin dhe luftimin e dhunës kundër grave dhe dhunës në familje. Shih: https://rm.coe.int/168046246b

Manual on Videoconferencing Legal and Practical Use in Criminal Cases, UN, New Yourk, 2017. Shih: https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/MANUAL_VIDEOCONFERENCING.pdf

Strategy on victims' rights (2020-2025), EU, Bruksel, 24.6.2020. Shih:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0258&from=EN.

Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU Policy Paper. Shih: https://www.ceps.eu/ëp-content/uploads/2021/05/Criminal-Justice-Fundamental-Rights-and-the-Rule-of-law-in-the-Digital-Age.pdf.

Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Këshilli i Evropës, 2000. Shih: https://rm.coe.int/09000016809e1154

Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons, UN, 2021. Shih: https://www.unodc.org/documents/treaties/ËG_TiP_2021/CTOC_COP_WG.4_2021_2/ctoc_cop_wg.4_2021_2_E.pdf

UN declaration of basic principles of justice for victims of crime and abuse of power

Ligje, akte nënligjore, studime dhe strategji

Ligji nr.7905, datë 21.3.1995 "Kodi i Procedures Penale i Rpublikës së Shqipërisë, i ndryshuar.

Ligji nr. 37/2017 "Kodi i Drejtësisë Penale për të Mitur.

Ligj nr. 8920 datë 11.7.2002 për ratifikimin e "Konventës së Kombeve të Bashkuara kundër krimit të organizuar ndërkombëtar" dhe dy protokolleve shtesë të saj.

Ligji nr.95/2016 "Për organizimin dhe funksionin e institucioneve për të luftuar korrupsionin dhe krimin e organizuar", neni 25.

Udhëzimi nr.8, datë 15.11.2021 i Prokurorit Përgjithshëm "Hetimi dhe ndjekja penale efektive të veprave penale me të mitur në konflikt me ligjin, fëmijët viktima dhe/ose dëshmitar".

Raport monitorimi

Analiza e Sistemit të Drejtësisë në Shqipëri, Qershor 2015, fq.149-150. http://www.reformanedrejtesi.al/sites/default/files/dokumenti_shqip_0.pdf.

Raport mbi gjetjet e monitorimit të përdorimit të sallave të gjyqit dhe sistemit të regjistrimit digjital audio në gjykata, raport i Komitetit Shqiptar të HeLsinkit, Tiranë 2017. https://ahc.org.al/ëp-content/uploads/2017/08/Raport-RDAcmyk_ValmiraOK-1.pdf

Strategjia e Drejtësisë për të Mitur, Raport monitorimi Janar- Dhjetor 2021, botim i Ministrisë së Drejtësisë, 2021.

Zbatimi i sistemit të menaxhimit të çështjeve civile/penale (CCMIS/ICMIS) pranë gjykatës së rrethit gjyqësor Tiranë, Durrës dhe Elbasan, raport monitorimi, ALTRI, 2018, f.18-19. Shih: https://altri.al/ëp-content/uploads/2018/05/Raport-Monitorimi-mbi-zbatimin-e-sistemit-CCMIS-ICMIS-1.pdf.

Vendime të GJEDNJ

Vendimi i GJEDNJ Eduardo González Nájera *kundër* Spanjës, aplikimi nr. 61047/13. Vendimi u aksesua në adresën: http://hudoc.echr.coe.int/webservices/content/pdf/001-141859?TID=ihgdqbxnfi.

Vendimi i GJEDNJ W.S. *kundër* Polonisë, 24.09.2007. Aplikimi nr. 21508/02. Vendimi u aksesua në adresën: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-81140%22ç}

Vendimi i GJEDNJ N.Ç. *kundër* Turqisë, aplikimi nr. 40591/1. Vendimi u aksesua në adresën: https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6931183-9316853%22ç}

Çështja Mraović *kundër* Kroacisë, aplikimi nr. 30373/13. Përmbledhje vendimi. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12787%22ç}

DILEMA KUSHTETUESE MBI DËNIMIN PENAL NË BASHKËPUNIMIN E POSAÇËM

FLORJAN KALAJA

1. Hyrje

Në cilësinë e gjyqtarit të deleguar për të gjykuar një çështje për llogari të Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit kam nisur një kontroll kushtetues incidental të paragrafit të parë të nenit 334 të Kodit Penal, konkretisht për pjesën që parashikohet dënimi fiks shtesë mbi veprën e kryer prej 5 vitesh burgim për pjesëmarrësit e organizatës kriminale apo grupit të strukturuar kriminal.[1] Ky punim është bazuar në të gjithë studimin dhe argumentet kushtetuese me anën e së cilave është konkluduar mbi atikushtetutshmërinë e nenit 334 të Kodit Penal, konkretisht mbi paragrafin e parë dhe të dytë të kësaj dispozite. Më tej shkrimi është pasuruar me argumentet doktrinare dhe jurisprudenciale respektive të përftuara dhe elaboruara gjatë studimit.

Shkrimi paraqet në mënyrë të përmbledhur edhe konkluzionet dhe arsyetimin e vendimmarrjes së Gjykatës Kushtetuese. Në shkrim kam argumentuar mbi gjithçka Gjykata Kushtetuese ka argumentuar në vendimmarrjen e saj. Më tej jam përpjekur të sygjeroj edhe zgjidhjet kushtetuese dhe ligjore interpretative në mënyrë që papajtueshmëria e formulimit të paragrafit të parë dhe të dytë të nenit 334 të Kodit Penal të mos rëndojë të drejtën për liri dhe siguri të subjekteve të gjykuar dhe të dënuar si pjesëtarë në formacionet kriminale të bashkëpunimit të posaçëm penal. Pikërisht këto janë konkluzionet dhe sygjerimet me të cilat përmbyllet shkrimi.

1 Shih Vendimin "*Për pezullimin e gjykimit dhe dërgimin e çështjes në Gjykatën Kushtetuese*" nr. 33 Regjistri Themeltar, datë 17.12.2021 të Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit.

2. Historiku i rregullimit normativ mbi bashkëpunimin e posaçëm në Shqipëri

Një kategorizim i përgjithshëm i llojeve të bashkëpunimit penal është ai që dallon bashkëpunimin e thjeshtë nga bashkëpunimi i posaçëm.[2] Tradicionalisht ligji penal shqiptar e ka bërë këtë ndarje. Kolegji Penal i Gjykatës së Lartë ka arsyetuar se, kur provohet se bashkëpunimi nuk ka qenë rastësor dhe ka kaluar marrëveshjen e thjeshtë, duke arritur kështu në një nivel organizimi strukturor të lartë dhe me një kompaktësi të qëndrueshme[3], që shkon në ngritjen e strukture vendimmarrëse dhe ekzekutuese në nivel hierarkik, kjo është e mjaftueshme për të konkluduar për ekzistencën në parim të bashkëpunimit të veçantë.[4] Pikërisht bashkëpunimi i posaçëm penal do të jetë objekti kryesor i analizës së këtij punimi, duke u përqendruar në mënyrën se si ligji penal material i posaçëm parashikon regjimin e përgjegjësisë penale.

Dy llojet e bashkëpunimit i gjejmë të rregulluara në Kodin Penal të Republikës Popullore të Shqipërisë[5] (në vijim Kodi Penal i vitit 1952). Në nenin 12 të këtij Kodi parashikohej se bashkëpunim quhet kryerja me dashje e një krimi nga disa persona bashkë ose krijimi për këtë qëllim i një organizate kriminale. Në paragrafin e dytë të nenit 14 parashikohej se në caktimin e dënimit për bashkëpunëtorët gjykata duhet të marrë parasysh shkallën dhe karakterin e pjesëmarrjes të secilit prej tyre në kryerjen e krimit. Ndërkohë në paragrafin e tretë të kësaj dispozite parashikohej se pjesëmarrësi i organizatës kriminale ka përgjegjësi penale jo vetëm për krimet në të cilat ai ka marrë pjesë drejtpërdrejtë por edhe për krimet e kryera nga pjesëmarrës të tjerë të organizatës kriminale, në qoftë se ka patur dijeni se kryerja e këtyre krimeve hynte në planin e veprimtarisë së organizatës kriminale.

Në pjesën e posaçme ky Kod parashikonte dy dispozita dhe vepra penale

---

2 "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia, faqe 481 - 481. Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 85.

3 Shih Udhëzimin nr. 1, datë 10.01.1966 të Pleniumit të Gjykatës së Lartë. Ndër të tjera në këtë Udhëzim arsyetohet se:

"*Grupi i organizuar dallohet nga bashkëpunimi i thjeshtë për faktin se tek ai ka një kompaktësi dhe qëndrueshmëri më të madhe midis pjesëtarëve të tij, si dhe një shkallë më të lartë organizimi në krahasim me bashkëpunimin e thjeshtë kur organizimi është i një shkalle më të ulët ose mungon fare.*"

4 Shih Vendimin Nr. 59000-01410-00-2012 i Regjistri Themeltar, Nr. 00-2014-1935 i Vendimit (175), datë 16.07.2014 i Kolegjit Penal të Gjykatës së Lartë.

5 Shih Ligjin nr. 1470, datë 23.05.1952 botuar në Gazetën Zyrtare nr. 15/1952. Sipas nenit 342 të këtij Kodi, ky ligj ka hyrë në fuqi me datë 01.09.1952.

me anën e të cilave dënohej organizimi apo pjesëmarrja në format e posaçme të bashkëpunimit penal. Neni 69 i Kodit Penal të vitit 1952, nën titullin "*Organizimi ose pjesëmarrja në bandat e armatosura*", parashikonte se:

"*Organizimi ose pjesëmarrja në bandat e armatosura që hyjnë në Republikën Popullore të Shqipërisë nga jashtë ose që formohen në tokën e Republikës Popullore të Shqipërisë për të minuar pushtetin popullor me anë sulmi kundër institucioneve shtetërore dhe shoqërore, ose kundër përfaqësuesve të pushtetit popullor, punonjësve shoqërorë ose qytetarëve të tjerë, ose me anë shkatërrimi ose dëmtimi të ndërmarrjeve dhe pasurisë shtetërore, shoqërore ose pasurisë së qytetarëve dënohen: me heqje lirie jo më pak se dhjetë vjet ose me vdekje dhe kurdoherë me konfiskimin e pasurisë.*"

Në nenin 76 të Kodit Penal të vitit 1952, nën titullin "*Pjesëmarrja në një organizatë kundër pushtetit popullor*", parashikohej se:

"*Pjesëmarrja në një organizatë kriminale e cila ka për qëllim kryerjen e krimeve kundër shtetit, të parashikuara nga nenet 64 gjer në 75 dhe nga neni 78 të Këtij Kodi, dënohet si krim i kryer në bazë të nenit që parashikon krimin.*"

Bashkëpunimi i zakonshëm dhe i posaçëm penal parashikohej dhe rregullohej edhe në Kodin Penal të Republikës Popullore Socialiste të Shqiqërisë[6] (në vijim Kodi Penal i vitit 1977). Në nenin 13 të këtij Kodi si formë e posaçme e bashkëpunimit njihej banda e armatosur dhe organizata kundërrevolucionare. Në nenin 15 të këtij Kodi përgjegjësia penale e bashkëpunëtorëve, atyre të bandës së armatosur dhe organizatës kundërrevolucionare rregullohej njëlloj sikurse në dispozitën analoge të Kodit Penal të vitit 1952.

Në pjesën e posaçme të Kodit Penal të vitit 1977 kishte dy dispozita të veçanta që parashikonin si vepër penale organizimin apo pjesëmarrjen në format e veçanta të bashkëpunimit. Në nenin 51, nën titullin "*Organizimi i bandave të armatosura ose pjesëmarra në to*", parashikohej se:

"*Organizimi i bandave të armatosura ose pjesëmarrja në këto banda, që hyjnë në Republikën Popullore Socialiste të Shqipërisë nga jashtë ose që formohen brenda vendit për të kryer krime kundër shtetit dënohen: me heqje të lirisë jo më pak se dhjetë vjet ose me vdekje.*"

Në nenin 57 të Kodit Penal të vitit 1977, nën titullin "*Krijimi i një*

6 Shih Ligjin nr. 5591, datë 15.06.1977, të ndryshuar me Ligjin nr. 6300, datë 27.03.1981. Sipas nenit 248 të këtij Kodi, ky ligj ka hyrë në fuqi me datë 01.10.1977.

organizate kundërrevolucionare ose pjesëmarrja në të", parashikohej se:

"*Krijimi i një organizate me karakter fashist, antidemokratik dhe antisocialist ose pjesëmarrja në të për të kryer krime kundër shtetit dënohen: me heqje të lirës jo më pak se dhjetë vjet ose me vdekje.*"

Në variantin fillestar të Kodit Penal në fuqi format e veçanta të bashkëpunimit penal kishin rregullime të ndryshme nga sa parashikohet sot dhe syresh atëbotë ishin vetëm dy. Neni 28 i Kodit Penal në variantin fillestar të hyrjes në fuqi dhe deri në vitin 2004, nën titullin "*Banda e armatosur dhe organizata kriminale*", parashikonte se:

"*Banda e armatosur dhe organizata kriminale përfaqësojnë forma të bashkëpunimit të veçantë që dallohen jo vetëm nga numri i pjesëmarrësve, por edhe nga shkalla e organizimit dhe e qëndrueshmërisë së tyre për kryerjen e një numri veprash penale.*

Organizata kriminale përfaqëson shkallën më të lartë të bashkëpunimit për kryerjen e veprimtarisë kriminale të qëndrueshme.

Krijimi dhe pjesëmarrja në bandë të armatosur dhe në organizata kriminale, si dhe kryerja e veprave penale prej tyre, cilësohen si vepra penale më vete dhe dënohen sipas parashikimeve të Pjesës së Posaçme të këtij Kodi.

Pjesëtarët e bandës së armatosur dhe të organizatës kriminale janë përgjegjës për të gjitha veprat penale të kryera nga banda dhe organizata, kur kanë vepruar si organizatorë, ekzekutorë, shtytës dhe ndihmës.

Pjesëtari i bandës së armatosur dhe i organizatës kriminale përjashtohet nga përgjegjësia penale për pjesëmarrjen në to kur pendohet dhe vihet në ndihmë të organeve kompetente për parandalimin e veprimtarisë dhe zbulimin e bashkëpunëtorëve.

Shërben si rrethanë për zbutjen e dënimit, dhe në raste të veçanta edhe për uljen e tij nën minimumin e parashikuar nga ligji, kur pjesëtari i bandës së armatosur dhe i organizatës kriminale që ka kryer vepra penale, pendohet dhe bashkëpunon me organet kompetente për zbulimin e veprimtarisë dhe bashkëpunëtorëve të tjerë.

Gjykata, kur çmon se roli i pjesëtarit të penduar të bandës së armatosur dhe të organizatës kriminale nuk është kryesor, kur veprat e kryera prej tij nuk janë me rrezikshmëri të theksuar dhe kur ndihma e dhënë për zbulimin e veprimtarisë dhe bashkëpunëtorëve të bandës apo organizatës kriminale është e rëndësishme, mund ta përjashtojë atë nga dënimi."

Neni 333 i Kodit Penal, nën titullin "*Krijimi i bandës së armatosur dhe organizatës kriminale*", nga hyrja në fuqi e deri para ndryshimeve ligjore të vitit 2004, parashikonte se:

"*Krijimi i bandës së armatosur apo organizatës kriminale ose pjesëmarrja në to, me qëllim për kryerjen e krimeve, dënohet nga pesë gjer në pesëmbëdhjetë vjet.*"

Neni 334 i Kodit Penal, nën titullin "*Kryerja e krimeve nga banda e armatosur dhe organizata kriminale*", nga hyrja në fuqi e Kodit Penal dhe deri në momentin kur hynë në fuqi ndryshimet ligjore të vitit 2004 parashikonte se:

"*I. Kryerja e krimeve nga banda e armatosur apo organizata kriminale do të dënohet sipas dispozitave penale përkatëse duke shtuar dënimin për krimin e kryer edhe me pesë vjet burgim të tjera, kur dispozita referuese përmban dënim me burgim dhe një lloj dënimi më i lehtë, por pa kaluar kufirin maksimal të dënimit me burgim.*

II. Kur dispozita përkatëse referuese përmban dënim me burgim apo me burgim të përjetshëm a me vdekje, dënohet me njëzet e pesë vjet burgim ose me burgim të përjetshëm a me vdekje.

III. Kur dispozita përkatëse referuese përmban vetëm dënim me burgim të përjetshëm a me vdekje, dënohet me burgim të përjetshëm a me vdekje."

Në vitin 1998 në Kodin Penal u prezantua një formë e posaçme e organizatës kriminale, konkretisht organizata kriminale e cila kultivon, prodhon, fabrikon apo trafikon lëndët narkotike.[7] Neni 284/a i Kodit Penal, nën titullin "*Organizimi dhe drejtimi i organizatave kriminale*", parashikon se:

"*Organizimi, drejtimi dhe financimi i organizatave kriminale me qëllim kultivimin, prodhimin, fabrikimin ose trafikun e paligjshëm të narkotikëve dënohet me burgim nga 10 deri në 20 vjet.*

Krijimi i kushteve apo lehtësirave për veprimtari të tilla nga persona me funksione shtetërore, dënohet me burgim nga 5 deri në 15 vjet."

Në vitin 2001, si pasojë e vendimit të Gjykatës Kushtetuese me të cilin u shfuqizua dënimi penal me vdekje, u shfuqizuan fjalët "*a me vdekje*" në nenin 334 të Kodit Penal.[8]

---

7 Ligjin nr. 8279, datë 15.01.1998 "*Për disa ndryshime e shtesa në ligjin nr. 7895, datë 27.01.1995 "Për Kodin Penal të Republikës së Shqipërisë*".

8 Shih Ligjin nr. 8733, datë 24.01.2001 "*Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë*

Në vitin 2002 Republika e Shqipërisë ka ratifikuar me ligj Konventën e Organizatës së Kombeve të Bashkuara Kundër Krimit të Organizuar Ndërkombëtar bashkë me dy protokollet shtesë të saj.[9] Pasi në shkronjën "a" dhe "c" të nenit 2 të kësaj Konvente jepet përkufizimi i formave të posaçme të bashkëpunimit penal, në nenin 5, nën titullin "*Penalizimi i pjesëmarrjes në një grup kriminal të organizuar*", parashikohet se çdo Shtet Palë duhet të adaptojë masa të tilla ligjore dhe masa të tjera që mund të konsiderohen të nevojshme për të cilësuar si vepra penale, në rastet kur kryhen qëllimisht:

a) secilin ose të dy prej rasteve të mëposhtme si vepra penale të dallueshme nga ato që përfshijnë tentativën ose kryerjen e aktivitetit kriminal:

(i) marrëveshjen me një ose disa persona të tjerë për të kryer një krim serioz për një qëllim që lidhet direkt ose jodirekt me marrjen e përfitimeve financiare ose materiale dhe, nëse kërkohet nga legjislacioni i brendshëm, që përfshin një veprim të ndërmarrë nga një prej pjesëmarrësve në zbatim të marrëveshjes, ose që përfshin një grup të organizuar kriminal;

(ii) veprimin e një personi, i cili, duke njohur qëllimin dhe aktivitetin e përgjithshëm kriminal të një grupi të organizuar kriminal ose synimin e tij për të kryer krimet në fjalë, merr pjesë aktivisht në:

(a) veprimtaritë kriminale të grupit të organizuar kriminal;

(b) Veprimtaritë e tjera kriminale të grupit të organizuar kriminal, duke ditur se pjesëmarrja e tij/saj do të kontribuojë në arritjen e qëllimit kriminal të përshkruar më lart;

(c) organizimin, drejtimin, dhënien e ndihmës, përkrahjen, lehtësimin ose dhënien e këshillave për kryerjen e një krimi serioz që përfshin një grup kriminal të organizuar.

Më tej në pikën 3 të kësaj dispozite parashikohet se Shtetet Palë, ligji i brendshëm i të cilëve kërkon përfshirjen e një grupi kriminal të organizuar për qëllimet e veprave penale të cilësuara si të tilla, në përputhje me paragrafin 1 (a) (i) të këtj neni, do të sigurojë që legjislacioni i tyre i brendshëm të mbulojë të gjitha krimet serioze që përfshijnë grupet e organizuara kriminale.

Duke pasur parasysh edhe detyrimet ndërkombëtare të marra përsipër sikurse u sollën në vëmendje më lart, në vitin 2004 Kodi Penal pësoi ndryshime

---

27.01.1995, "Kodi Penal i Republikës së Shqipërisë".

9 Shih Ligjin nr. 8920, datë 11.7.2002 "*Për ratifikimin e "Konventës së Kombeve të Bashkuara Kundër Krimit të Organizuar Ndërkombëtar" dhe dy Protokolleve shtesë të saj*".

të rëndësishme në drejtim të rregullimit normativ penal të bashkëpunimit të posaçëm.[10] Në Nenin 28 i Kodit Penal pas këtyre ndryshimeve ligjore u parashikua se:

- *Organizata kriminale është forma me e lartë e bashkëpunimit, në të cilin bëjnë pjesë tre ose më shumë persona dhe që dallohet nga shkalla e veçantë e organizimit, strukturimit, qëndrueshmërisë, kohëzgjatjes, si dhe nga qëllimi për kryerjen e një a më shumë veprave penale, për të realizuar përfitime materiale dhe jomateriale.*
- *Organizata kriminale, për realizimin e qëllimeve të saj, përdor forcën, mjetet e tjera të kërcënimit, nënshtrimin dhe heshtjen për shkak të pjesëmarrjes dhe veprimtarisë se saj, për të kryer vepra penale, për të siguruar, në çdo mënyrë, administrimin ose vënien nën kontroll të veprimtarive ekonomike, të koncesioneve, autorizimeve, sipërmarrjeve dhe shërbimeve publike, për të realizuar përfitime ose avantazhe të padrejta për vete a personat e tjerë ose për të ndaluar a penguar ushtrimin e lirë të së drejtës së votës gjatë fushatave zgjedhore, si dhe veprimtarive të tjera të ngjashme me to.*
- *Organizata terroriste është një formë e veçantë e organizatës kriminale, që synon kryerjen e veprimeve të dhunshme për qëllime terroriste, si përmbysje të rendit kushtetues, turbullim të rëndë të rendit publik, ngjallje të frikës dhe të pasigurisë në masë.*
- *Banda e armatosur është një formë e veçantë bashkëpunimi që, duke zotëruar armë, municione luftarake dhe mjete të tjera të nevojshme, synon kryerjen e veprave penale, të parashikuara në krerët V, VI dhe VII të pjesës së posaçme të këtij Kodi.*
- *Grupi i strukturuar kriminal është formë e veçantë bashkëpunimi, në të cilin bëjnë pjesë tre ose me shumë persona, për kryerjen e një a më shumë veprave penale, për të realizuar përfitime materiale dhe jomateriale.*
- *Grupi i strukturuar kriminal për kryerjen e një vepre penale nuk formohet rastësisht e nuk është e nevojshme të dallohet për anëtarësi të qëndrueshme, ndarje detyrash, organizim dhe strukturim te zhvilluar.*
- *Krijimi dhe pjesëmarrja në një organizate kriminale, organizate terroriste, bandë të armatosur ose grup të strukturuar kriminal cilësohen si vepra penale dhe dënohen sipas parashikimeve të pjesës*

10 Shih Ligjin Nr. 9275, datë 16.9.2004 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar.

se posaçme të këtij Kodi ose të dispozitave të tjera penale të veçanta.

- *Anëtarët e organizatës kriminale, të organizatës terroriste, bandës së armatosur ose grupit të strukturuar kriminal janë përgjegjës për të gjitha veprat penale, të kryera prej tyre, në përmbushjen e qëllimeve të veprimtarisë së tyre kriminale.*
- *Pjesëtari i organizatës kriminale, organizatës terroriste, bandës së armatosur ose i grupit të strukturuar kriminal; përfiton përjashtimin nga dënimi ose uljen e tij, kur jep ndihmesë, që gjykohet vendimtare për njohjen e veprimtarisë së tyre, të bashkëpunëtorëve të tjerë, pasurive të zotëruara drejtpërdrejt ose jo prej tyre, si dhe për veprimtaritë hetimore, që zhvillohen ndaj organizatave kriminale, organizatave terroriste, bandave të armatosura dhe grupeve të strukturuara kriminale.*"[11]

Në ndërhyrjen ligjore të vitit 2004 u prezantuan edhe tre dispozita ligjore rishtare, të cilat formësuan tre figura veprash penale të posaçme. Kështu u shtua neni 234/a i Kodit Penal me titull "*Organizata terroriste*" me përmbajtje si vijon:

"*Krijimi, organizimi, drejtimi dhe financimi i organizatës terroriste dënohen me burgim jo me pak se pesëmbëdhjete vjet.*

Pjesëmarrja ne organizata terroriste dënohet me burgim nga shtate deri ne pesëmbëdhjete vjet."

Më tej, nën titullin "*Banda e armatosur*", në nenin 234/b të Kodit Penal u parashikua se:

"*Krijimi, organizimi, drejtimi dhe financimi i bandës së armatosur dënohen me burgim nga dhjetë deri në pesëmbëdhjete vjet.*

Pjesëmarrja në bandën e armatosur dënohet me burgim nga pesë deri në dhjetë vjet."

Në nenin 333 të Kodit Penal, nën titullin "*Organizata kriminale*", me

11 Shih Vendimin Nr. 59000-01410-00-2012 i Regjistri Themeltar, Nr. 00-2014-1935 i Vendimit (175), datë 16.07.2014 i Kolegjit Penal të Gjykatës së Lartë. Ndër të tjera është arsyetuar se:

"*...me ligjin nr.9275 datë 16.09.2004, nuk ka asnjë ndryshim në lidhje me kuptimin ligjor të "bandës së armatosur", si formë e veçantë bashkëpunimi, kjo formë e bashkëpunimit mbetet e njëjtë, ashtu si para këtyre ndryshimeve, por, me qëllim për të shmangur çdo lloj interpretimi, atë që para ndryshimeve të bëra me këtë ligj, pra, sqarimin e konceptit të "bandës së armatosur", si formë e veçantë bashkëpunimi, e bënte, rast pas rasti, praktika gjyqësore dhe doktrina juridike, pas këtyre ndryshimeve kuptimin e këtij koncepti e ka bërë vetë ligji, konkretisht, pika 3 e nenit 28 të Kodit Penal.*"

ndryshimet ligjore të vitit 2004 u parashikua se:

"*Krijimi, organizimi ose drejtimi i organizatave kriminale dënohen me burgim nga pesë deri në pesëmbëdhjetë vjet.*

Pjesëmarrja në një organizatë kriminale dënohet me burgim nga katër deri në tetë vjet.

Nëse organizata kriminale është e armatosur dhe pjesëtarët e saj zotërojnë armë dhe lëndë shpërthyese për qëllime të përmbushjes së veprimtarisë së saj kriminale, edhe nëse ato janë të fshehura ose të mbajtura në vende të veçanta, dënimi me burgim shtohet me një të tretën.

Kur veprimtaritë ekonomike, të ndërmarra ose të kontrolluara nga pjesëtarë të organizatës kriminale, financohen tërësisht ose pjesërisht me produkte të veprave penale, masa e dënimit, sipas paragrafëve të sipërpërmendur në këtë nen, shtohet me një të tretën deri në një të dytën e tij."

Më tej në nenin 333/a, nën titullin "*Grupi i strukturuar kriminal*", u parashikua se:

"*Krijimi, organizimi ose drejtimi i një grupi të strukturuar kriminal për kryerjen e veprave penale dënohen me burgim nga tre deri në tetë vjet.*

Pjesëmarrja në grupin e strukturuar kriminal dënohet me burgim nga dy deri në pesë vjet."

Në vitin 2007 u shfuqizua paragrafi i dytë i pikës së parë të nenit 28 të Kodit Penal. Ndërkohë përmes kësaj ndërhyrje legjislative u ndryshua pika e dytë e kësaj dispozite me këtë përmbajtje:

"*2. Organizata terroriste është një formë e veçantë e organizatës kriminale, e përbërë nga dy ose më shumë persona, që kanë një bashkëpunim të qëndrueshëm në kohë, me synim kryerjen e veprave me qëllime terroriste.*"[12]

3. Natyra juridike e veprave penale formale të bashkëpunimit të posaçëm

Të gjitha këto vepra penale janë kriminalizimi i formave të posaçme të bashkëpunimit, të cilat, ndryshe nga bashkëpunimi i thjeshtë i cili është episodik, aksidental apo rastësor[13], paraqiten në formacione shoqërore

12 Shih Ligjin nr. 9686, datë 26.2.2007 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar."

13 Shih Vendimin nr. 28252, datë 07.06.2017 të Seksionit Penal IV të Gjykatës së Kasacionit të Republikës së Italisë.

të strukturuara dhe të qëndrueshme në kohë. Qëllimi unik kriminal dhe marrëveshja e këtyre formacioneve është filli që shpjegon të gjithë aktivitetin penal në kohë dhe në hapësirë.[14] Është pikërisht kjo lidhje sistematike dhe e qëndrueshme e anëtarësisë në formacione të tilla shoqërore kriminale arsyeja që ligjvënësi i ka vlerësuar se vetëm formësimi i tyre cenon sigurinë e rendit publik dhe autoritetin e shtetit, duke i penalizuar sakaq me titull të posaçëm si figura veprash penale, pavarësisht aktivitetit kriminal të kryer.[15]

Sikurse kuptohet nga leximi i dispozitave të sjella në vëmendje më lart, secila nga këto figura veprash penale, qoftë krijimi, organizimi, drejtimi, financimi dhe pjesëmarrja në organizatën terroriste, bandën e armatosur apo grupin e strukturuar kriminal janë vepra penale formale[16]. Kjo do të thotë se për ekzistencën e tyre nuk kërkohet vërtetimi i një pasoje materiale kriminale dhe se mjafton vërtetimi objektivisht i këtyre formave të kriminalitetit që parashikohet në hipotezat e normave.[17]

Gjithashtu secila nga këto figura të veprave penale për nga ana objektive se si realizohet klasifikohet si vepër penale e qëndrueshme[18], vazhdueshme dhe latente në kohë. Sipas paragrafit të pestë të nenit 28 të Kodit Penal, mjafton krijimi dhe pjesëmarrja në një organizate kriminale, organizate terroriste, bandë të armatosur ose grup të strukturuar kriminal, që këto fakte të cilësohen si vepra penale më vete dhe që për rrjedhojë të dënohen sipas parashikimeve të pjesës se posaçme të këtij Kodi ose të dispozitave të tjera penale të veçanta. Për ta përditësuar këtë normë me karakter të përgjithshëm neni 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal kanë parashikuar figura konkrete veprash penale dhe dënimet respektive për to.

---

14 Shih Vendimin nr. 36131, datë 25.08.2014 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

15 Shih Vendimin datë 22.01.1997 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

16 Shih Vendimin nr. 14, datë 17.04.2007 të Gjykatës Kushtetuese. Në këtë vendim Gjykata Kushtetuese arsyeton ndër të tjera se: "*Siç pranohet edhe në doktrinën e të drejtës penale, në këndvështrimin e pasojave kriminale, në varësi të qenies ose jo të pasojës si element i figurës së veprës penale, këto të fundit, ndahen në materiale dhe formale. Duke e analizuar në këtë vështrim figurën e veprës penale që parashikon neni 284/a, mund të konkludohet se ajo, përfshihet në figurat formale të veprave penale, gjë që do të thotë se kjo vepër konsiderohet e kryer që nga momenti i organizimit dhe i pjesëmarrjes në organizatën kriminale pavarësisht nga ardhja e pasojave. Kur nga veprimtaria e organizatës kriminale kanë ardhur edhe pasoja, atëherë veprat penale do të konkurrojnë.*"

17 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, 103.

18 Shih "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia, faqe 499.

Këto norma ligjore që rregullojnë përgjegjësinë penale për organizimin kolektiv të individëve në format e posaçme të bashkëpunimit penal synojnë të garantojnë sigurinë dhe rendin juridik publik dhe realizimin e të drejtës kushtetuese për organizim kolektiv të individëve për qëllime të ligjshme, sipas nenit 9, 46 dhe 47 të Kushtetutës. Veprat penale formale dhe latente që penalizojnë organizimet kolektive të paligjshme të individëve e marrin legjitimitetin kushtetues të ngritjes në nivelin e krimeve të rënda vetëm për faktin se ato venë në rrezik sigurinë kombëtare dhe rendin juridik publik, rrezik i cili prezumohet vetëm nga ekzistenca e organizimeve të tilla kolektive.[19]

Ky regjim i veçantë i garant i sigurisë publike së shtetit kryen një funksion mbrojtës paraprak për vlera kaq themelore që qëndrojnë në themelin e ndërtimit të shoqërisë, të cilat ligjvënësit i interesojnë që t'i neutralizojë që në gjenezën e tyre. Në doktrinën e së drejtës penale këto krime konsiderohen si krime të rrezikut apo vepra penale të cunguara[20] dhe se ato ndikojnë edhe në legjitimitetin kushtetues të organizimeve kolektive të individëve si një nga të drejtat themelore me karakter social dhe politik.[21] Këto janë vepra penale përjashtim nga rregulli i përgjithshëm, pasi për nga alarmi social që përcjellin dhe për nga rrezikshmëria shoqërore dhe publike që kanë legjislatori ka kriminalizuar edhe fazën e përgatitjes së veprës penale.[22]

Organizimi i kësaj mënyre paraqet krijimin e mekanizmave paralel shtetëror, që shpërfillin ekzistencën, organet dhe rregullat normative, duke krijuar sakaq një pushtet paralel apo "shtet brenda shtetit" në territorin ku ato veprojnë dhe mbi veprimtarinë që ato kryejnë.[23]

Kusht për kualifikimin juridik të ekzistencës së tyre është predispozita e një strukture të organizuar që lejon realizimin e programit apo planit kriminal që ky organizim synon.[24] Karakteristika kryesore e bashkëpunimit

19 Shih Vendimin nr. 30791, datë 17.07.2013 të Seksionit VI Penal të Gjykatës së Kasacionit të Republikës së Italisë.

20 "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia, faqe 500 - 501.

21 Shih "*Codice Penale Operativo, annotato con dottrina e giurisprudenza*", I Codici Simone OP3, a cura di Luciano Ciafardini, Mario Formisano, Rocco Pezzano, Paolo Scognamiglio, XVII Edizione 2021, Edizioni Giuridiche Simone, faqe 1299.

22 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 3.

23 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, 91.

24 Shih Vendimin nr. 27433/2017 të Seksionit Penal VI të Gjykatës Supreme të Kasacionit të Republikës së Italisë.

të posaçëm është shumësia e kualifikuar personave aktiv që konsumojnë veprën penale të dakordësuar për pjesëmarrje dhe për kryerjen e aktivitetit kriminal dhe se në çdo rast marrëveshja e arritur ndërmjet tyre ka karakter të qëndrueshëm për bashkëkontribut reciprok në arritjen e qëllimeve kriminale.[25]

Në çdo rast ana subjektive e krijimit, organizimit, drejtimit, financimit apo pjesëmarrjes në këto forma të posaçme të bashkëpunimit penal është kryerja e një aktiviteti kriminal homogjen apo heterogjen, i cili mund të kryet pjesërisht apo jo.[26] Në çdo rast përmes këtyre veprave penale konsiderohet krim i perfeksionuar vetëm pjesëmarrja, pavarësisht nga realizimi i aktivitetit kriminal të programuar.[27] Ana subjektive e krijimit të formave të posaçme të bashkëpunimit është element konstitutiv i veprave penale të parashikuara në nenin 234/a, 234/b, 333 dhe 333/a të Kodit Penal dhe nëse nuk vërtetohet elementi subjektiv i qëllimit të posaçëm për kryerjen e një apo më shumë veprave atëherë vetëm plotësimi i elementeve të anës subjektive nuk mjafton për të konkluduar se ekzistojnë këto vepra penale.[28] Ndërgjegja dhe vullneti i dijenisë së pjesëmarrjes dhe kontributit të bashkëpunëtorit në bashkëpunimin e posaçëm është elementi që provon dashjen dhe konstituon sakaq anën subjektive të këtyre krimeve.[29]

Një model i tillë i penalizmit të krijimit të këtyre formave të posaçme të bashkëpunimit penal gjendet i rregulluar edhe në nenin 74 (*organizata kriminale e narkotikëve*) të Dekretit të Presidentit të Republikës së Italisë nr. 309/1990[30], nenin 270 (*organizata puçiste*), nenin 270-*bis* (*organizata*

25 Shih Vendimin nr. 28252/2017 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

26 Shih Vendimin nr. 19198, datë 21.04.2017 të Seksionit Penal III të Gjykatës së Kasacionit të Republikës së Italisë. Shih gjithashtu edhe Vendimin nr. 42635, datë 03.11.2004 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë. Përmes kësaj jurisprudence realizohet dallimi ndërmjet marrëveshjes së thjeshtë (*pactum sceleris*) dhe marrëveshjes së posaçme (*pactum societatis*) për kryerjen e aktivitetit kriminal.

27 Shih Vendimin nr. 7187, datë 19.02.2004 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

28 Shih Vendimin Nr. 59000-01410-00-2012 i Regjistri Themeltar, Nr. 00-2014-1935 i Vendimit (175), datë 16.07.2014 i Kolegjit Penal të Gjykatës së Lartë, paragrafi 210.

29 Shih Vendimin nr. 456, datë 21.09.2012 të Seksionit Penal VI "*Cena ed altri, Rv. 254225*"; Vendimin nr. 1147, datë 19.11.2007 të Seksionit Penal VI "*Stabile, Rv. 238403*"; Vendimin nr. 41717, datë 06.11.2006 të Seksionit Penal VI "*Geraci, Rv. 235589*" të Gjykatës së Kasacionit të Republikës së Italisë. "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia, faqe 492, 493, 496, 498 – 499.

30 Shih Dekretin e Presidentit të Republikës së Italisë nr. 309, datë 09.10.1990, akt normativ i cili ka hyrë në fuqi me datë 15.11.1990. Shih në web Fletoren Zyrtare: https://www.gazzettaufficiale.it/eli/id/1990/10/31/090G0363/sg.

terroriste), nenin 306 dhe 307 (*banda e armatosur*)[31] apo në nenin 416 apo 416-*bis* (*organizata mafioze*) të Kodit Penal të Republikës së Italisë.[32] Nga jurisprudenca e Gjykatës së Kasacionit të këtij shteti pranohet se perfeksionimi i këtyre veprave penale konsiderohet juridikisht i kryer në momentin dhe në vendin në të cilin nis ekzistenca e këtyre organizatave apo në momentin kur ato janë gati për të nisur veprimtarinë[33], pasi në këtë moment vlerësohet nga ligjvënësi se ka lindur rreziku real që kërkojnë normat penale të mos ekzistojë për sigurinë e shtetit dhe shoqërisë[34]. Krime të tilla konsiderohen nga kjo jurisprudencë si vepra penale me rrezik të prezumuar[35] dhe të cilat synojnë të mbrojnë paraprakisht marrëdhënien juridike që kanë si objekt[36].

Nga ana tjetër kjo jurisprudencë ka pranuar se fundi i konsumimit të këtyre veprave penale formale dhe latente ndodh kur merr fund marrëveshja për të bashkëpunuar apo kur arrestohen apo ndalohen personat bashkëpunëtorë deri në numrin inferior ligjor kur formalisht nuk mund të ketë më formë të posaçme të bashkëpunimit penal.[37] Në të njëjtën mënyrë është konkluduar nga kjo jurisprudencë se edhe dënimi penal me burgim e ndërpret bashkëpunimin e posaçëm penal në raport me të dënuarin, duke i dhënë sakaq fund ekzistencës së kësaj vepre penale për të.[38] Si rregull përjashtohet ekzistenca e tentativës në kryerjen e këtyre veprave penale, duke qenë se konsiderohet se ato janë vepra penale rreziku dhe se përmes tyre kriminalizohet faza më e hershme e

31 Shih në web: https://www.altalex.com/documents/news/2014/07/14/dei-delitti-contro-la-personalita-dello-stato. Vizituar me datë 02.01.2022.

32 Shih në web: https://www.altalex.com/documents/news/2014/04/18/dei-delitti-contro-l-ordine-pubblico. Vizituar me datë 02.01.2022.

33 Shih Vendimin nr. 44369, datë 24.10.2014 të Seksionit Penal V dhe Vendimin nr. 49995, datë 31.10.2017 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

34 Shih Vendimin nr. 45388, datë 07.12.2005 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë.

35 Shih Vendimin nr. 10.12.1990 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë.

36 Shih Vendimin datë 27.02.1989 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë. Për organizatën terroriste shih Vendimin nr. 2651, datë 21.01.2015 të Seksionit Penal V; Vendimin nr. 10380, datë 08.03.2019 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë.

37 Shih Vendimin datë 07.12.1979 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë.

38 Shih Vendimin nr. 17265, datë 24.04.2008 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë (për organizatën mafioze).

Shih gjithashtu "*Codice Penale Operativo, annotato con dottrina e giurisprudenza*", I Codici Simone OP3, a cura di Luciano Ciafardini, Mario Formisano, Rocco Pezzano, Paolo Scognamiglio, XVII Edizione 2021, Edizioni Giuridiche Simone, faqe 710 (për organizatën puçiste). Shih gjithashtu Vendimin nr. 10380, datë 08.03.2019 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë (për organizatën terroriste).

mundshme e veprës penale.[39]

Këto fakte penale kanë një rrezikshmëri shoqërore të veçantë. Ligjvënësi ka krijuar prokurori dhe gjykata të posaçme për ushtrimin e ndjekjes penale dhe gjykimin e tyre, duke pasur parasysh rëndësinë e madhe që ka realizimi i drejtësisë në këtë fushë të posaçme të së drejtës. Megjithatë ligjvënësi nuk është mjaftuar me kaq në penalizmin dhe dekurajimin e formave të veçanta të bashkëpunimit penal. Në nenin 334 të Kodit Penal, nën titullin "*Kryerja e veprave penale nga organizata kriminale dhe grupi i strukturuar kriminal*", u realizuan këto ndryshime:

"*Kryerja e veprave penale nga pjesëtarë te organizatës kriminale dhe të grupit të strukturuar kriminal dënohet sipas dispozitave penale përkatëse, duke i shtuar dënimit për veprën penale të kryer edhe pesë vjet burgim, si dhe gjobën në masën një të tretën, por pa kaluar kufirin maksimal të dënimit me burgim.*"

Sikurse kuptohet nga leximi i kësaj dispozite të ndryshuar dhe në gjendjen e saj sikurse është në fuqi sot[40], veç dënimit penal që do të individualizohet për secilin pjesëtar të organizatës kriminale dhe grupit të strukturuar kriminal sipas meritës, sipas nenit 27 të Kodit Penal[41], dhe veç dënimit që këto bashkëpunëtorë do të marrin për krijimin apo pjesëmarrjen në një nga format e bashkëpunimit të posaçëm penal, gjykata e posaçme do të duhet të shtojë edhe 5 vjet burgim, nëse vepra penale e kryer dënohet me burgim, apo edhe një të tretën e gjobës, nëse vepra penale e dhënë dënohet me apo edhe me burgim. Në çdo rast si kusht për gjykatën e posaçme mbetet që, dënimi i

39 Shih Vendimin nr. Datë 07.04.1989 të Seksionit Penal I dhe Vendimin nr. 4294, datë 29.01.2015 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë.

40 Kjo dispozitë sot formulohet:

"*1. Kryerja e veprave penale nga pjesëtarë të organizatës kriminale dhe të grupit të strukturuar kriminal dënohet sipas dispozitave penale përkatëse, duke i shtuar dënimit për veprën penale të kryer edhe pesë vjet burgim, si dhe gjobën në masën një të tretën, por pa kaluar kufirin maksimal të dënimit me burgim.*

2. Kur dispozita përkatëse referuese përmban dënim me burgim apo me burgim të përjetshëm, dënohet me njëzet e pesë vjet burgim ose me burgim të përjetshëm.

3. Kur dispozita përkatëse referuese përmban vetëm dënim me burgim të përjetshëm, dënohet me burgim të përjetshëm."

41 Kjo dispozitë parashikon se:

"Organizatorët, shtytësit dhe ndihmësit kanë përgjegjësi si edhe ekzekutorët për veprën penale të kryer prej tyre.

Në caktimin e dënimit për bashkëpunëtorët, gjykata duhet të mbajë parasysh shkallën e pjesëmarrjes së secilit dhe rolin e luajtur në kryerjen e veprës penale."

individualizuar për veprën penale të kryer dhe shtesa e dënimit për kryerjen e veprës penale në kuadrin e organizatës kriminale apo grupit të struktura kriminal, nuk duhet të kalojë kufirin maksimal të dënimit me burgim.

Në fakt një model i tillë rregullimi ligjor për ndëshkimin e dyfishtë të të njëjtit fakt nuk gjendet në legjislacionin Italian, legjislacion ky që ka shërbyer si model në hartimin e normave penale materiale të posaçme për ndëshkimin e krimeve të rrezikut të prezumuar, sikurse janë neni 234/a, 234/b, 333 dhe 333/a të Kodit Penal. Një model i tillë nuk rrjedh as nga detyrimet ndërkombëtare të marra përsipër me ligj nga Republika e Shqipërisë, sipas nenit 5 të Kushtetutës. Sikurse shikohet, një model i tillë ligjor i penalizmit të dyfishtë nuk është marrë as nga trashëgimia e ligjeve penale ndër vite.

4. Problematikat e zbatimit të nenit 334 të Kodit Penal

Sikurse mund të kuptohet nga leximi i kësaj dispozite, ka elemente të pamjaftueshëm të teknikës legjislative në formulimin e rregullit normativ që do të duan përgjigje në praktikën e zbatimit të ligjit penal. Kjo është e meta më e vogël që kjo dispozitë penale ka.

Problemi i parë që kjo dispozitë tregon është fakti se nuk është gjithëpërfshirëse për të gjitha format e bashkëpunimit të posaçëm penal. Duke qenë se në nenin 28 të Kodit Penal ravijëzohen katër forma të bashkëpunimit të posaçëm penal, konkretisht organizata kriminale, organizata terroriste, banda e armatosur dhe grupi i strukturuar kriminal, do të duhej që të katër këto forma të posaçme bashkëpunimi të njiheshin si anë objektive dhe anë subjektive e posaçme e kryerjes së veprave penale, gjë që do të mundësonte zbatimin e shtesës së dënimit me burgim apo me gjobë, sipas nenit 334 të Kodit Penal.

Nga leximi i nenit 334 të Kodit Penal në lidhje me nenin 28 të këtij Kodi, kuptohet se vetëm kryerja e veprave penale të kuadër të organizatës kriminale, organizatës terroriste si formë e posaçme e organizatës kriminale dhe kryerja e vepra penale në kuadrin e grupit të strukturuar kriminal mundet të legjitimojë gjykatën e posaçme të zbatojë shtesën e dënimit me burgim me 5 vjet dhe të dënimit me gjobë me një të tretën. Duhet të mbahet parasysh se banda e armatosur është një formë e veçantë e bashkëpunimit të posaçëm penal dhe se si e tillë nuk mund të përfshihet as në organizatën kriminale dhe as në grupin e strukturuar kriminal.[42] Banda e armatosur në këtë kuptim të

42 Shih Vendimin Nr. 59000-01401-00-2010 i Regj. Themeltar, Nr. 00-2014-1115 i Vendimit (48), datë 24.02.2014 të Kolegjit Penal të Gjykatës së Lartë.

përcaktimeve ligjore është e ndryshme nga organizata kriminale dhe se këto dy forma të posaçme bashkëpunimi nuk mundet të bashkekzistojnë në një formacion të caktuar kriminal dhe në të njëjtën kohë, pasi ato janë të tilla që përjashtojnë njëra tjetrën si forma të paligjshme organizimi.[43] Sipas pikës 3 të nenit 28 të Kodit Penal, qëllimi i këtij lloj formacioni të paligjshëm është gjithmonë kryerja e vepra penale kundër rendit kushtetues, cenimit të pavarësisë së vendit, veprat me qëllime terroste apo veprat që cenojnë marrëdhëniet me shtetet e tjera.

Kjo do të thotë se kryerja e veprës penale në kuadër të bandës së armatosur, si formë e posaçme e bashkëpunimit penal, nuk do të mund të sjellë shtesën e dënimit me gjobë apo me burgim sipas nenit 334 të Kodit Penal.[44] Ky konkluzion përforcohet më shumë nga garancia kushtetuese e nenit 29 të Kushtetutës, konventore e nenit 7 të KEDNJ dhe garancia ligjore e pamundësimit të zbatimit të ligjit penal me analogji e parashikuar në nenin 3 të Kodit Penal.

Për rrjedhojë konstatohet se neni 334 i Kodit Penal nuk ka respektuar nenin 18 të Kushtetutës për të trajtuar në mënyrë të barabartë përgjegjësinë penale të shtuar të pjesëmarrësve të bandës së armatosur sikurse rregullon përgjegjësinë penale të shtuar të pjesëmarrësve të organizatës kriminale apo grupit të strukturuar kriminal. Nga ana tjetër mosrespektimi i nenit 18 të Kushtetutës lidhur me barazinë e shtetasve përballë përgjegjësisë penale që shkaktojnë veprimet e tyre ka krijuar edhe një ndërhyrje paradoksale në ligj, pasi një formë e posaçme bashkëpunimi më e lehtë në kryerjen e veprave penale, sikurse është grupi i strukturuar kriminal në raport me bandën e armatosur, merr sipas ligjit përgjegjësi penale më të madhe se sa një formë më e rëndë e bashkëpunimit penal të posaçëm. Kjo nuk mund dhe nuk duhet të ndodhë, duke pasur parasysh nenin 17 dhe 18 të Kushtetutës.

Problemi i dytë që ka kjo dispozitë është fakti që nuk ka një limit maksimum të shtesës së gjobës me një të tretën e masës së caktuar të saj si dënim penal për një vepër penale konkrete. Ndërkohë që për dënimin me burgim parashikohet se shtesa e dënimit nuk duhet të kalojë maksimumin e dënimit me burgim, ligji penal hesht për kufirin maksimal që mund të përshkojë shtesa e dënimit me gjobë. Sigurisht që fjalët "*me burgim*" në paragrafin e parë të nenit 334 të Kodit Penal janë të tepërta dhe të pavend dhe se pika si shenjë pikëzimi në këtë paragraf duhet të ishte vendosur pas shprehjes

43 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, faqe 108, 112.

44 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, 157.

"*të dënimit*". Megjithatë vlerësohet se kjo mangësi e teknikës legjislative duhet dhe mund të kalohet me interpretim gjyqësor të harmonizuar, duke konkluduar se edhe maksimumi i dënimit me gjobë, sipas nenit 34 të Kodit Penal, nuk mund të kalohet në rastin e zbatimit të nenit 334 të Kodit Penal.

Problemi i tretë që ka kjo dispozitë është fakti se paragrafi i dytë i saj nuk është përditësuar ndër vite me ndryshimet që ka pësuar pjesa e përgjithshme e Kodit Penal, konkretisht e dënimit me burgim. Kjo dispozitë për herë të fundit është ndryshuar në vitin 2004 dhe se në këtë kohë neni 32 i Kodit Penal parashikonte se dënimi me burgim për krimet mund të jepej nga pesë ditë deri në 25 vjet. Ndërkohë në vitin 2013 u ndryshua paragrafi i parë i nenit 32 të Kodit Penal, duke u parashikuar dënimi me burgim për krimet nga pesë ditë deri në 35 vjet. Paragrafi i dytë i nenit 334 të Kodit Penal nuk u përditësua me këtë ndryshim të rëndësishëm të dënimit me burgim[45] dhe se edhe sot kjo dispozitë lexohet si vijon:

"*Kur dispozita përkatëse referuese përmban dënim me burgim apo me burgim të përjetshëm, dënohet me njëzet e pesë vjet burgim ose me burgim të përjetshëm.*"

Deri në vitin 2013 gjykata e krimeve të rënda kishte si mundësi vetëm dy lloje dënimesh për këto vepra penale. Së pari caktimin e dënimit maksimal me burgim, që do të thotë me 25 vjet burgim. Së dyti caktimin e dënimit me burgim të përjetshëm. Ndërkohë ndryshimet ligjore të vitit 2013 e bën pa kuptim lidhëzën "*ose*" të përdorur nga paragrafi i dytë i nenit 334 të Kodit Penal dhe njëkohësisht edhe qëllimin e legjislatorit që e pasur që në momentin kur Kodi Penal ka hyrë në fuqi. Sot interpretimi harmonizues i paragrafit të dytë të nenit 334 të Kodit Penal me paragrafin e parë të nenit 32 të këtij Kodi bën që lidhëza literalisht e përdorur "*ose*" nga ligjvënësi të lexohet juridikisht "*deri*" nga gjykatat. Për rrjedhojë do të duhet të konkludohet se në këto raste gjykata mund të përcaktojë si dënim me burgim masën nga 25 vjet deri në 35 vjet ose dënimin me burgim të përjetshëm.

Problemi i katërt që ka kjo dispozitë është humbja e koherencës dhe e utilitetit të paragrafit të tretë të nenit 334 të Kodit Penal. Prej kohësh ky paragraf ka mbetur rudiment. Kjo pjesë e dispozitës parashikon një eventualitet që nuk është i mundur, konkretisht parashikimin nga ana e ligjvënësit si sanksion vetëm të një nga dënimet kryesore, konkretisht dënimin me burgim apo thënë ndryshe parashikimin e një dënimi fiks për një vepër penale. Një teknikë e tillë legjislative është e pamundur kushtetutshmërisht dhe konvencionalisht

45 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, faqe 158.

që të ndodhë, pasi nëse do të ndodhnin do të dhunonin Kushtetutën dhe KEDNJ.

Problemi i gjashtë që ka kjo dispozitë është përcaktimi i dënimit fiks me burgim apo me gjobë. Në këtë rast legjislatori ka parashikuar se çdo vepër penale e kryer në kuadër të organizatës kriminale apo grupit të strukturuar kriminal, veç dënimit të caktuar për të nga gjykata e posaçme, merr edhe një dënim shtesë fiks prej pesë vitesh dhe një dënim me gjobë shtesë fiks me një të tretën vetëm për faktin se është kryer në kuadrin e një nga tre formave të posaçme të bashkëpunimit penal. Thënë ndryshe, kryerja e veprës penale si pjesëtar i organizatës kriminale, organizatës terroriste apo grupit të strukturuar është një rrethanë rënduese që merr një dënim fiks prej pesë vitesh burgim dhe një të tretën shtesë të masës së caktuar të gjobës. Kjo do të thotë se bashkëpunimi i posaçëm penal, sipas shkronjës "gj" të nenit 50 të Kodit Penal, merr automatikisht pesë vjet burgim dhe një të tretën e masës së gjobës mbi dënimin e individualizuar për veprën penale të kryer.

Problemi i shtatë që kjo dispozitë ka lidhet me paragrafin e dytë. Leximi dhe zbatimi i paragrafit të dytë të nenit 334 sikurse është shkruar nga ligjvënësi do të thotë se, nëse ligji penal material i posaçëm parashikon dënim me burgim për një vepër penale, kur kjo vepër kryhet në kuadër të njërës prej formave të bashkëpunimit të posaçëm që kjo dispozitë citon, atëherë vepra e kryer dënohet me burgim me njëzet e pesë vjet burgim ose me burgim të përjetshëm. Një parashikim i tillë vjen haptazi në kundërshtim me nenin 17 të Kushtetutës dhe krijon sanksione haptazi joproporcionale penale lidhur me përgjegjësinë penale të autorëve të veprave penale, pasi çdo vepër penale për të cilën ligji penal material i posaçëm parashikon vetëm dënimin me burgim, pavarësisht se çfarë sanksionesh parashikon ajo dispozitë, vetëm kryerja e veprës penale nën një formë bashkëpunimi të posaçëm i ndryshon sanksionet ligjore nga 25 vjet burgim deri në dënimin me burgim të përjetshëm. Thënë konkretisht, edhe pse një vepër penale në ligj dënohet deri në dhjet vjet burgim, fakti që kjo vepër është kryer në kuadrin e një forme të posaçme bashkëpunimi bën të mundur që kjo vepër penale të dënohet me burgim 25 vjet apo me burgim të përjetshëm. Një parashikim i tillë ligjor apo për më tepër një zbatim i tillë i këtij parashikimi ligjor është haptazi jologjik, jokushtetues, joproporcional apo i padrejtë. Në literaturën juridike të së drejtës penale materiale në Shqipëri ka edhe mendime se kjo pjesë e dispozitës ligjore e shndërron atë në një normë të pazbatueshme dhe të pakuptueshme për urdhërimin ligjor që ligjvënësi ka dashur të japë.[46]

46 Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, 158 - 159.

Problemi i tetë mundet të vijë në interpretimin e kundërt të problematikës së shtatë të trajtuar më lart. Sipas mënyrës që është rregulluar paragrafi i dytë i nenit 334 të Kodit Penal probleme mundet të krijohen në rastet kur një vepër penale, e cila parashikon dënim në minimumin e saj mbi 25 vjet burgim, kryhet në kuadër të një nga format e posaçme të bashkëpunimit. Pyetja që do të shtrohet është se kush do të ketë në këtë rast minimumi i sanksionit ligjor, 25 vjet burgim, sikurse parashikon paragrafi i dytë i nenit 334 të Kodit Penal, apo mbi 25 vjet burgim, sikurse parashikon vepra penale e posaçme? Sigurisht, duke pasur parasysh parashikimin e nenit 29 të Kushtetutës, nenit 7 të KEDNJ apo nenit 3 të Kodit Penal, do të konkludonim se në këtë rast kryerja e veprës penale në kuadrin e bashkëpunimit të posaçëm do të dënohet në minimumin e saj me 25 vjet burgim. Por kjo zgjidhje krijon paradoksin e paragrafit të dytë të nenit 334 të Kodit Penal, pasi nga ky parashikim ligjor del se kryerja e veprës penale në kuadrin e bashkëpunimit të posaçëm dënohet më pak se kryerja e veprës penale në bashkëpunimin e thjeshtë apo edhe se kryerja e saj individualisht. Kjo është e papranueshme.

Problemi i nëntë që kjo dispozitë ka është dhunimi i parimit kushtetues të mos dënimit dy herë për të njëjtin fakt penal (*ne bis in idem*), sipas nenit 34 të Kushtetutës. Konstatohet se ligjvënësi drejtimin, organizimin, financimin dhe pjesëmarrjen në organizatën kriminale, organizatën terroriste dhe grupin e strukturuar kriminal e ka parashikuar si vepër penale formale dhe latente dhe e ka dënuar me sanksione të larta duke e shquar kurdoherë si krim (shih nenin 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal).

Njëkohësisht kryerjen e veprave penale nën këto forma të posaçme bashkëpunimi e ka dënuar me dënimin fiks me burgim prej 5 vitesh dhe me dënimin fiks me gjobë prej një të tretën, sipas nenit 334 të Kodit Penal. Kjo do të thotë se individi që kryen vepër penale si pjesë e organizatës kriminale, organizatës terroriste dhe grupit të strukturuar kriminal dënohet fillimisht si pjesëtar i këtyre formave të posaçme bashkëpunimi dhe më tej edhe pse kanë kryer vepra penale në këto forma të posaçme bashkëpunimi, pa përfshirë sakaq dënimin që ato do të marrin për veprën penale të kryer. Kjo do të thotë se bashkëpunimi i posaçëm kriminal në këto raste është dënuar dy herë nga ligji penal si fakt, duke ardhur sakaq në kundërshtim me nenin 34 të Kushtetutës dhe me ndalesën e parimit *ne bis in idem* në kuptimin substancial të tij.

Problemi i dhjetë që kjo dispozitë mbart në vetvete është i mënyrës së si është hartuar nën këndvështrimin e teknikës legjislative. Kjo dispozitë nuk parashikon vepër penale të posaçme dhe asnjë figurë konkrete të veprës penale. Kjo dispozitë ka karakter të përgjithshëm dhe rregullon mënyrën e

caktimit të dënimit për një nga elementet që ligji shquan si rrethanë rënduese në kryerjen e një apo disa veprave penale. Kjo do të thotë se dispozita nuk ka vend që të qendrojë në pjesën e posaçme të Kodit Penal. Ajo ka rregulluar ekskluzivisht një çështje të pjesës së përgjithshme të Kodit Penal dhe se natyra juridike e saj kërkonte që ligjvënësi ta kishte përfshirë si rregullim në pjesën materiale të rregullimeve të përgjithshme të korpusit më të rëndësishëm normativ penal.

Kjo dispozitë ngjan me rregullimet e pjesës së përgjithshme të Kodit Penal të Republikës së Italisë, konkretisht në pjesën që rregullohen rrethanat rënduese apo lehtësuese të bashkëpunimit penal, të cilat shërbejnë për shtimin e dënimit apo për uljen e tij nën disa hapësira limit minimale dhe maksimale që ky ligj ka parashikuar.[47] Për rrjedhojë vlerësoj se neni 334 i Kodit Penal nuk e ka vendin në pjesën e posaçme të Kodit Penal. Kjo dispozitë duhet të ishte parashikuar dhe vendosur menjëherë pas nenit 28 të Kodit Penal dhe nën një rregullim normativ tjetër, që do të mundësonte shuarjen e çdo problematike që është paraqitur më lart dhe që do të analizohet në vijim.

5. Praktika gjyqësore mbi zbatimin e nenit 334 të Kodit Penal

Në gjykatat e posaçme penale ndër vite ka pasur dy qëndrime jurisprudenciale mbi përcaktimin dhe individualizimin e dënimit penal për veprat penale të kryera në kuadër të bashkëpunimit të posaçëm. Qëndrimi i parë ka rezultuar të jetë gjithmonë shumica vendimmarrëse. Qëndrimi i dytë interpretativ ka rezultuar të jetë gjithmonë qëndrim i një pakice gjyqtarësh.

Shumica e gjyqtarëve dhe praktika e vazhdueshme gjyqësore e gjykatës së shkallës së parë[48], gjykatës së apelit[49] apo e Kolegjit Penal të Gjykatës së

47 Shih për shembull nenin 112 dhe vijues të Kodit Penal të Republikës së Italisë.

48 Shih për shembull Vendimin nr. 50, datë 29.07.2008; Vendimin nr. 11, datë 16.02.2009; Vendimin nr. 43, datë 13.07.2009; Vendimi nr. 69, datë 23.11.2009; Vendimin nr. 45, datë 27.07.2011; Vendimin nr. 135, datë 03.12.2015 të Gjykatës së Shkallës së Parë për Krimet e Rënda. Shih gjithashtu Vendimin nr. 1, datë 16.01.2012; Vendimin nr. 62, datë 23.04.2018 të Gjykatës së Shkallës së Parë për Krimet e Rënda.

Shih gjithashtu edhe Vendimin nr. 39, datë 18.05.2021; Vendimin nr. 45, datë 14.06.2021 i Gjykatës së Posaçme të Shkallës së Parë Kundër Krimit të Organizuar dhe Korrupsionit.

49 Shih për shembull Vendimin nr. 66, datë 17.11.2008; Vendimin nr. 36, datë 26.09.2009; Vendimin nr. 50, datë 29.07.2008; Vendimin nr. 61, datë 24.12.2010; Vendimi nr. 37, datë 02.10.2010; Vendimin nr. 20, datë 25.03.2011; Vendimin nr. 62, datë 07.11.2011; Vendimin nr. 75, datë 06.12.2012; Vendimin nr. 10, datë 10.02.2016; Vendimin nr. 69, datë 19.09.2018 të Gjykatës së Apelit për Krimet e Rënda.

Lartë[50] ka qenë se bashkëpunimi i posaçëm penal dënohet si vepër penale më vete, vepër penale e cila është formale dhe latente kohë kohë. Në këtë qëndrim arsyetohet se mjafton drejtimi, krijimi, organizimi, financimi apo

Shih gjithashtu edhe Vendimin nr. 62, datë 23.04.2018 të Gjykatës së Shkallës së Parë për Krimet e Rënda i cilin është lënë në fuqi me Vendimin nr. 69, datë 19.09.2018 të Gjykatës së Apelit për Krimet e Rënda.

Shih gjithashtu edhe Vendimin nr. 20, datë 25.03.2011 të Gjykatës së Apelit për Krimet e Rënda. Shih gjithashtu Vendimin nr. 45, datë 02.07.2012 të Gjykatës së Apelit për Krimet e Rënda.

Shih gjithashtu Vendimin nr. 75, datë 06.12.2012 të Gjykatës së Apelit për Krimet e Rënda. Ndër të tjera në këtë vendim arsyetohet se: "*Gjykata vlerëson se nenet 333 e 334, si dispozita të pjesës së posaçme të Kodit Penal, konkurrojnë me njëra tjetrën, ato aplikohen sipas rastit, sipas veprimtarisë kriminale të të pandehurve që bëjnë pjesë në krimin e organizuar. Nëse të pandehurit, kanë kryer edhe vepra referuese penale, si në rastin në gjykim atë të "Ndihmës për kalim të paligjshëm të kufirit", dënimi edhe për nenet 333/a edhe sipas nenit 334 të K.Penal, nuk përbën cenim të parimit "ne bis in idem".*"

50 Shih Vendimin Nr. 56550-00591-00-2016 Regjistri Themeltar, Nr. 00-2017-8 i Vendimit (3), datë 01.02.2017 të Kolegjit Penal të Gjykatës së Lartë; Vendimin Nr. 56550-00582-00-2009 i Regj. Themeltar, Nr.00-2010-283 i Vendimit (22), datë 20.01.2010 të Kolegjit Penal të Gjykatës së Lartë; Vendimin Nr.56550-00145-00-2011 i Regj. Themeltar, Nr. 00-2013-987 i Vendimit (197), datë 12.06.2013 të Kolegjit Penal të Gjykatës së Lartë; Vendimin nr. Nr.56260-00039-00-2012 i Regj. Themeltar, Nr.00-2013-1550 i Vendimit (200), datë 12.06.2013; Vendimin Nr. 59000-01401-00-2010 i Regj.Themeltar, Nr.00-2014-1115 i Vendimit (48), datë 24.02.2014 të Kolegjit Penal të Gjykatës së Lartë.

Shih gjithashtu Vendimin Nr. 56550-00843-00-2009 i Regj. Themeltar, Nr. 00-2010-354 i Vendimit (226), date 10.03.2010 të Kolegjit Penal të Gjykatës së Lartë. Në këtë vendim Kolegji Penal i Gjykatës së Lartë arsyeton se:

"*Gjithashtu ky Kolegj çmon se vlen të tërhiqet vëmendja dhe t'i bëhet vërejtje trupit gjykues së Gjykatës së Apelit për Krimet e Rënda në lidhje zbatimin e ligjit material penal, përsa i përket mosdënimit të të gjykuarve për nenin 333/a të K.Penal.*

Nëse do t'i referohemi elementeve të veprës penale të "Grupi i strukturuar kriminal", i parashikuar nga neni 333/a i K.Penal, e në veçanti paragrafit të dytë të kësaj dispozite, subjekt i kësaj vepre penale është pjesëmarrësi në grupin e strukturuar kriminal, për të cilin ligjvënësi ka parashikuar dënim të veçantë. Pra një i pandehur dënohet për kryerjen e kësaj vepre penale (pjesëmarrje në grupin e strukturuar kriminal), pavarësisht nëse ai kryen apo jo ndonjë vepër penale në funksion të krijimit të këtij grupi. Ndërkohë që në ligjin penal është parashikuar se, nëse pjesëmarrësi në grupin e strukturuar kriminal, çdo lloj bashkëpunëtori, organizator, ndihmës, etj, kryen vepra penale në kuadër të këtij lloj bashkëpunimi të veçantë, atëherë ai dënohet sipas sanksioneve të parashikuara në nenin 334/1 të K.Penal. Vlerësojmë se janë të gabuara arsyetimet dhe këndvështrimi i Gjykatës së Apelit për Krime të Rënda në rastin konkret, kur thotë se: "nuk konkurrojnë veprat penale të parashikuara nga nenet 333/a dhe 334 të K.Penal kur ekzistojnë të dyja veprat, pra pjesëmarrja në grupin e strukturuar kriminal dhe kryerja e pjesëmarrësit në këtë grup e veprave penale, por autori i veprës penale "Grupi i strukturuar kriminal" dënohet për kryerjen e këtij krimi, vetëm atëherë kur ai nuk ka konsumuar ndonjë vepër penale si anëtar i këtij grupi". Konkluzione të tilla të këtij trupi gjykues vijnë në kundërshtim si me vetë përcaktimet e dispozitave të ligjit material penal (neneve 28 pika 5, 333/a, 334 të K.Penal), por edhe me qëndrimet e mëparshme të vetë kësaj gjykate."

Së fundmi shih Vendimin Nr. 56550-01298-2016 i Regj. Themeltar, Nr. 00-2021-18 i Vendimit, datë 15.01.2021 të Kolegjit Penal të Gjykatës së Lartë.

pjesëmarrja në organizatën kriminale, organizatën terroriste, organizatën kriminale të narkotikëve, bandën e armatosur apo grupin e strukturuar kriminal për të konkluduar se është perfeksionuar konsumimi i veprës penale të parashikuar nga neni 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal. Më tej bashkëpunëtorët janë deklaruar fajtor dhe janë dënuar për veprat penale të kryera, sipas dispozitës apo dispozitave penale të posaçme të cilat parashikojnë këto vepra dhe paragrafit të dytë të nenit 27 të Kodit Penal. Pika 5 e nenit 28 të Kodit Penal është interpretuar në vijimësi së fillimisht penalizon veprën penale formale dhe të qëndrueshme në kohë, respektivisht sipas nenit 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal, dhe më tej dënon me shtesën e dënimit respektive, sipas nenit 334 të Kodit Penal, çdo vepër të kryer në kuadër të bashkëpunimit të posaçëm. Dënimi i marrë për veprën penale formale bashkohet me dënimin e marrë për veprën penale konkrete të kryer, sipas rregullave të nenit 55 të Kodit Penal. Ndërkohë shtesa e dënimit sipas nenit 334 të Kodit Penal bashkohet aritmetikisht me dënimin e caktuar për veprën penale.

Në këtë linjë arsyetimi dhe qëndrimi mbi zbatimin kumulativisht të dispozitave të posaçme penale ka pasur edhe qëndrime që e kanë konsideruar nenin 334 të Kodit Penal si vepër penale e posaçme, konkretisht si vepra penale e kryerjes së veprave penale si pjesëmarrës në organizatën kriminale, organizatën terroriste apo në grupin e strukturuar kriminal.[51] Edhe sipas kësaj praktike gjyqësore dënimet për veprën, për llojin e bashkëpunimit të posaçëm dhe për kryerjen e veprës penale në një nga format e bashkëpunimit të posaçëm bashkohen kumulativisht.

Nga ana tjetër ka ekzistuar edhe një qëndrim pakice e gjyqtarëve lidhur me zbatimin e nenit 334 në raport me nenin 234/a, 284/a, 333 dhe 333/a

51 Shih Vendimin nr. 11, datë 16.02.2009; Vendinin nr. 48, datë 15.12.2010; Vendimin nr. 39, datë 25.05.2012; Vendimin nr. 135, datë 03.12.2015 të Gjykatës së Shkallës së Parë për Krimet e Rënda. Shih Vendimin nr. 39, datë 25.05.2012 të Gjykatës së Shkallës së Parë për Krimet e Rënda.

Shih gjithashtu edhe Vendimin Nr. 56550-00582-00-2009 i Regj. Themeltar, Nr.00-2010-283 i Vendimit (22), datë 20.01.2010 të Kolegjit Penal të Gjykatës së Lartë. Në këtë vendim merret e mirëqenë se neni 334 i Kodit Penal është vepër penale më vete dhe se në këtë vendim, duke qenë se u konkludua se nuk ka bashkëpunim të posaçëm por ka bashkëpunim të thjeshtë, u pushua çështja penale për akuzat ndaj të pandehurve sipas nenit 334 të Kodit Penal.

Shih gjithashtu edhe Vendimin Nr. 56550-00435-00-2009 i Regj. Themeltar, Nr.00-2010-480 i Vendimit (200), datë 03.03.2010 të Kolegjit Penal të Gjykatës së Lartë.

Shih gjithashtu edhe Vendimin Nr.56550-00145-00-2011 i Regj. Themeltar, Nr.00-2013-987 i Vendimit (197), datë 12.06.2013 të Kolegjit Penal të Gjykatës së Lartë, paragrafi 29, 31, 33.

të Kodit Penal.[52] Sipas këtij qëndrimi, nuk mund të zbatohen të dy këto dispozita dënimesh penale në një rast të caktuar, pasi do të cenohej parimi *ne bis in idem* në kuptimin material, sipas nenit 34 të Kushtetutës.[53] Kjo

52 Shih për shembull Vendimin nr. 57, datë 13.10.2009; Vendimin nr. 41, datë 10.07.2009 të Gjykatës së Apelit për Krimet e Rënda.

53 Shih për shembull Vendimin nr. 62, datë 07.11.2011 të Gjykatës së Apelit për Krimet e Rënda. Ndër të tjera në këtë vendim arsyetohet se:

"*Vendimi i gjykatës së shkallës së parë në tërësinë e tij është i drejtë, ndërkohë që nuk është i tillë për rastin kur ka vleresuar se njëkohësisht me veprat e kryera nga të pandehurit në bashkëpunim të veçantë, sipas nenit 28/4 të Kodit Penal, konkuron edhe vepra e "Grupi i strukturuar kriminal" sipas nenit 333/a të Kodit Penal. Në këtë konkluzion ky kolegj del për shkak të parashikimit të pikës 5 të nenit 28 të Kodit Penal që referon në nenin 333/a (dhe 333) të Kodit Penal, ballafaquar me nenin 334 të po këtij Kodi. Kështu ndërsa "Krijimi dhe pjesëmarrja në një organizatë kriminale, organizatë terroriste, bandë të armatosur ose grup të strukturuar kriminal" cilësohen si vepra penale dhe dënohen sipas parashikimeve të pjesës së posaçme të këtij Kodi (pika 5, neni 28 i K.Penal), që është pikërisht neni 333 dhe 333/a i Kodit Penal, kur pjestari i organizates kriminale apo i grupit të strukturuar kriminal kryen vepër penale tjetër apo të ndryshme nga ajo e krijimit dhe pjesëmarrjes në organizatë kriminale apo grup të strukturuar kriminal dënohet sipas dispozitave penale përkatëse të vepres së kryer, duke i shtuar këtij dënimi edhe pesë vjet burgim, si dhe gjobën në masën një të tretën (pika 1, neni 334 të K.Penal), ose me 25 vjet burgim (pika 2, neni 334 të K.Pr. Penale) apo me burgim të përjetshëm (pika 3, neni 334 të K.Penal). Pra, kur ende veprimi "bashkëpunues i veçantë" i krijimit apo pjesemarrjes ne organizate kriminale apo grup të strukturuar kriminal nuk është konkretizuar në kryerjen e një tjetër vepre penale, gjen vend sipas rastit aplikimi i nenit 333 apo 333/a i Kodit Penal. Ndërsa kur veprimi "bashkëpunues i veçantë" i krijimit apo pjesëmarrjes në organizatë kriminale apo grup të strukturuar kriminal konkretizohet në kryerjen e një tjetër vepre penale, ai thithet dhe nuk konkurron, duke u dënuar personi për veprën penale të kryer si edhe për veprimet e "bashkëpunimit të veçantë", sipas rastit, me dënimin e parashikuar nga njëra prej pikave të nenit 334 të Kodit Penal. Që nëse do të bënim një paralelizëm, do të ishte njësoj si rasti i "armëmbajtjes pa leje" (neni 278 të K.Penal) me "vjedhjen me armë" (140 të K.Penal), ku e para nuk konkurron dhe thithet nga e dyta. Krimi i "Grupi i strukturuar kriminal" (neni 333/a të K.Penal) është një vepër penale e qëndrueshme, ku i vetëm ai është i ndëshkueshëm penalisht, por nëse ai shoqëron një tjetër vepër penale, zbatimi, i nenit 334 të K.Penal mbi vepren e kryer, bën të thithet ai.*

Në të kundërt, ashtu siç ka vlerësuar gjykata e shkallës së parë, është e qartë se të pandehurit e lartpërmendur kanë marrë dy herë dënim për të njëjtin veprim të "bashkëpunimit të veçantë", gjë që bie në kundërshtim me parashikimin kushtetues se "Askush nuk mund të dënohet më shumë se një herë për të njëjtën vepër penale" (neni 34 i Kushtetutës)."

Ky vendim rezulton të jetë rekursuar. Kolegji Penal i Gjykatës së Lartë me Vendimin nr. Nr.56260-00039-00-2012 i Regj. Themeltar, Nr.00-2013-1550 i Vendimit (200), datë 12.06.2013. Ndër të tjera në këtë vendim është arsyetuar se:

"*Ky qëndrim i Gjykatës së Apelit për Krime të Rënda nuk mbështetet në legjislacionin penal në fuqi, duke bërë interpretim me analogji të ligjit penal, në kundërshtim me praktikën*

linjë arsyetimi përpiqet të gjejë një interpretim pajtues të zbatimit të nenit 334 të Kodit Penal në raport me nenet 234/a, 284/a, 333 dhe 333/a të këtij Kodi. Sipas këtij qëndrimi, neni 234/a, 284/a, 333 dhe 333/a i Kodit Penal do të mund të zbatohen për sa kohë bashkëpunëtorët në bashkëpunimin e posaçëm penal nuk kryejnë vepra penale në kuadrin e formave të posaçme të bashkëpunimit. Në momentin kur ato kryejnë vepra penale në kuadrin e formave të posaçme të bashkëpunimit penal, atëherë bashkëpunëtorët nuk do të mbajnë më përgjegjësi penale sipas nenit 234/a, 284/a, 333 dhe 333/a të Kodit Penal por dënimi i tyre do të shtohet sipas nenit 334 të Kodit Penal.[54] Në këtë mënyrë sipas kësaj linje arsyetimi mund të zgjidhet respektimi i parimit *ne bis in idem* në zbatimin e ligjit penal material të posaçëm.

Kjo linjë arsyetimi ka gjetur mbështetje edhe nga një qëndrim i mbajtur në Kolegjin Penal të Gjykatës së Lartë në vitin 2015. Përmes kësaj praktike gjyqësore është konkluduar se neni 234/a, 284/a, 333 dhe 333/a të Kodit Penal do të gjejnë zbatim vetëm për sa kohë nuk është kryer prej pjesëtarit të një nga format e bashkëpunimit të posaçëm një vepër penale në kuadër të këtij bashkëpunimi dhe në momentin kur kryhet një vepër penale konkrete atëherë këto dispozita thithen nga dënimi i shtuar sipas nenit 334 të Kodit Penal.[55]

---

e konsoliduar tashmë në këtë drejtim.

Vepra penale e krijimit dhe pjesëmarrjes në grupin e strukturuar kriminal e parashikuar nga neni 333/a i Kodit Penal, konkurron me veprat e tjera të kryera nga ana e grupit të strukturuar kriminal dhe nuk përthithet nga këto vepra."

54 Shih mendimin e gjyqtarit në pakicë në Vendimin "*Për pezullimin e gjykimit dhe dërgimin e çështjes në Gjykatën Kushtetuese*" nr. 33 Regjistri Themeltar, datë 17.12.2021 të Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit.

Shih gjithashtu Vendimin Nr. 59000-01373-00-2011 i Regj.Themeltar, Nr. 00-2013-1741 i Vendimit (315), datë 22.11.2012 i Kolegjit Penal të Gjykatës së Lartë.

55 Shih Vendimin nr. Nr. 59000-00240-00-2013 Regj. Themeltar, Nr. 00-2015-585 i Vendimit (38), datë 11.03.2015 i Kolegjit Penal të Gjykatës së Lartë. Ndër të tjera në këtë vendim arsyetohet se:

"*Kështu, ndërsa "krijimi dhe pjesëmarrja në një organizatë kriminale, organizatë terroriste, bandë të armatosur ose grup të strukturuar kriminal" cilësohen si vepra penale dhe dënohen sipas parashikimeve të pjesës së posaçme të këtij Kodi (pika 5, neni 28 i K.Penal), që është pikërisht neni 333 dhe 333/a i Kodit Penal. Pra është rasti kur pjesëtari i organizatës kriminale apo i grupit të strukturuar kriminal kryen vepër penale tjetër apo të ndryshme nga ajo e krijimit dhe pjesëmarrjes në: organizatë kriminale apo grup të strukturuar kriminal dënohet sipas dispozitave penale përkatëse të veprës së kryer, duke i shtuar këtij dënimi edhe pesë vjet burgim (pika 1, neni 334 të K.Penal), ose me 25 vjet burgim (pika 2, neni 334 të K.Pr.Penale) apo me burgim të përjetshëm (pika 3, neni 334 të K.Penal).*

Pra, bëhet fjalë për situatën, kur ende veprimi "bashkëpunues i veçantë" i krijimit

Interesant është fakti se edhe të vetmet praktika të Kolegjit Penal të Gjykatës së Lartë që ka përkrahur qëndrimin e përthithjes së veprave penale të parashikuara nga neni 234/a, 284/a, 333 dhe 333/a nga neni 334 i Kodit Penal nuk është respektuar në rigjykim nga ana e Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit në rigjykimin e po të njëjtës çështje.[56] Jo vetëm kaq, por edhe vetë Kolegji Penal i Gjykatës së Lartë në fillimin e vitit 2021 ka konfirmuar praktikën gjyqësore të saj të mbajtur në vazhdimësi mbi këtë çështje, duke konkluduar se veprat penale 234/a, 284/a, 333 dhe 333/a të Kodit Penal konkurrojnë me nenin 334 të Kodit Penal.[57]

---

apo pjesëmarrjes në organizate kriminale apo grup të strukturuar kriminal nuk është konkretizuar në kryerjen e një tjetër vepre penale, gjen vend sipas rastit aplikimi i nenit 333/a i Kodit Penal. Ndërsa kur veprimi "bashkëpunues i veçantë" i krijimit apo pjesëmarrjes në organizatë kriminale apo grup të strukturuar kriminal konkretizohet në kryerjen e një tjetër vepre penale, ai thithet dhe nuk konkurron, duke u dënuar personi për veprën penale të kryer si edhe për veprimet e "bashkëpunimit të veçantë", sipas rastit, me dënimin e parashikuar nga njëra prej pikave të nenit 334 të Kodit Penal.

Kolegji Penal i Gjykatës së Lartë vëren se krimi i "Grupi i strukturuar kriminal" (neni 333/a të K.Penal) është një vepër penale e qëndrueshme, ku i vetëm ai është i ndëshkueshëm penalisht, por nëse ai shoqëron një tjetër vepër penale, zbatimi, i nenit 334 të K.Penal mbi veprën e kryer, bën të thithet ai."

56 Shih Vendimin nr. 37, datë 18.04.2016 të Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit. Ndër të tjera në këtë vendim gjykata ka arsyetuar se: '*Vepra penale "Grup i strukturuar kriminal" është një vepër penale formale, që nënkuton se i pandehuri dënohet për kryerjen e kësaj vepre penale, pavarësisht nëse kryen apo jo ndonjë vepër penale konkrete, në funksion të krijimit të këtij grupi. Por, duhet saktësuar momenti kur fillon ajo vepër penale, nga momenti kur fillon kryerja e një vepre të caktuar/konkrete në kuadrin e grupit të strukturuar kriminal. Ligji material penal parashikon shprehimisht, që kur pjestarët e grupit të strukturuar, qofshin këto organizatoret apo pjesëmarrës të thjeshtë, kryejnë vepra penale në kuadrin e këtij grupi, në funksion të qëllimit për të cilin ai është krijuar, ateherë zbatohen sanksionet e parashikuara në nenin 334 të K.Penal. Por, në vlerësimin e gjykatës së apelit, kjo nuk mund ta përjashtojë të pandehurin nga përgiegjësia penale për për krijimin organizimin apo drejtimin apo pjesëmarrjen në një grup të strukturuar kriminal, ndërsa vet ligji penal përcakton secilen nga këto forma të tij, si penalisht të dënueshme. Dënimi për këtë vepër penale lidhet me kohën para se të fillojë aktiviteti kriminal i grupit, me kryerjen e veprave konkrete për cilën ky grup i strukturuar është krijuar - pra perkon me fazën para fillimit të aktivitetit të grupit, kur ai krijohet për një qëllim të caktuar kriminal. Në vlerësimin dhe në interpretimin e gjykatës së apelit, është kjo arsyeja që legjislatori e ka parashikuar këtë vepër penale më vete*."

57 Shih Vendimin Nr. 56550-01298-2016 i Regj. Themeltar, Nr. 00-2021-18 i Vendimit, datë 15.01.2021 të Kolegjit Penal të Gjykatës së Lartë. Në këtë vendim, pasi merret i drejtë dhe i bazuar në ligj arsyetimi i gjykatës së apelit (shih paragrafin 49), arsyetohet ndër të tjera: "50. Vepra penale e krijimit dhe pjesëmarrjes në grupin e strukturuar kriminal e parashikuar nga neni 333/a i Kodit Penal, konkurron me veprat e tjera të kryera nga ana e grupit të strukturuar kriminal dhe nuk përthithet nga këto vepra. (shih vendimin e Kolegjit Penal nr. 200, datë 12.06.2013, të Kolegjit Penal të Gjykatës së Lartë) Për këto arsye, të pandehurit do të përgjigjen

Kjo mënyrë e interpretimit të pakonkurueshmërisë dhe përthithjes së veprave penale formale të rrezikut nga neni 334 i Kodit Penal mbahet edhe nga një pjesë e mendimit juridik doktrinar në Shqipëri. Në mbajtjen e këtij qëndrimi referohet pikërisht në një nga praktikat e Kolegjit Penal të Gjykatës së Lartë, konkretisht në Vendimin nr. 38/2015.[58]

Ndërkohë së fundmi në gjykatat penale të posaçme është krijuar edhe një linjë e tretë e praktikës gjyqësore. Sipas kësaj linje arsyetimi, konkretisht kontesti kushtetues që është iniciuar prej këtij punimi, vlerësohet se nuk ekziston mundësia e interpretimit pajtues të dispozitave të posaçme materiale penale, konkretisht ndërmjet dispozitave 234/a, 284/a, 333 dhe 333/a me nenin 334 të Kodit Penal. Në këtë vlerësim ligjor konkludohet se nuk ka kuptim të arrihet në përfundimin se veprat penale formale dhe latente të parashikuara nga neni 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal do të ekzistojnë vetëm për sa kohë bashkëpunimi i posaçëm penal nuk zhvillon aktivitet kriminal konkret. Këto vepra penale kanë karakter të dyfishtë dhe të njëkohshëm, konkretisht janë formale dhe të shtrira në kohë për sa kohë ekziston forma e posaçme e bashkëpunimit. Nga ana tjetër nuk bën asnjë kuptim juridik që të konkludohet se kryerja e një vepre penale konkrete humb me fuqi prapavepruese apo retrospektive veprën penale formale të perfeksionuar juridikisht dhe të konsumuar sakaq. Nën të njëjtën linjë sikurse është zhvilluar edhe jurisprudenca e Gjykatës së Kasacionit të Republikës së Italisë e treguar më lart, nga ky qëndrim i tretë i praktikës gjyqësore vlerësohet se fundi i këtyre veprave penale latente është fundi i pjesëmarrjes në këto forma të bashkëpunimit të posaçëm apo prishja e bashkëpunimit dhe jo kryerja e veprave penale të tjera në kuadër të tyre apo për të cilat ato janë formuar.

Gjithashtu nuk bën asnjë kuptim juridik që veprat penale të parashikuara në nenin 234/a, 234/b, 284/a, 333 dhe 333/a të Kodit Penal, në momentin që kryhet një vepër penale konkrete dhe materiale nga bashkëpunëtorët, të përthithen nga dënimi i shtuar që parashikohet në nenin 334 të Kodit Penal. Nuk mundet që dënimi me burgim që parashikohet nga ligji, konkretisht nga

për veprën penale konkrete të kryer prej tyre, në rastin konkret vepra penale "Ndihma për kalim të paligjshëm kufiri" më shumë se një herë, e kryer në kuadër të grupit të strukturuar kriminal si dhe për veprën penale "Grupi i strukturuar kriminal" pasi këto janë veprat penale që ata kanë konsumuar nga ana objektive në rastin konkret."

58 "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia, faqe 499. Shih "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020, faqe 2, 155 -156, i cili i referohet ndër të tjera edhe Vendimit nr. 315, datë 21.11.2012 të Kolegjit Penal të Gjykatës së Lartë. Ky qëndrim në mendimin juridik është arsyetuar se duhet të ndiqet për të mos dhunuar parimin e "*res judicata*".

2 vjet deri në 30 vjet burgim të përthithet apo të minimizohet në një dënim 5 vjet burgim. Kjo linjë e arsyetimit juridik në praktikën gjyqësore arrin paradoksalisht në konkluzionin se vetëm bashkëpunimi i posaçëm penal në vetvete është më i rrezikshëm shoqërisht dhe për rrjedhojë më shumë i dënueshëm në rastin kur nuk kryen vepra penale se sa në rastin kur kryen veprat penale për të cilat ato forma bashkëpunimi të posaçëm penal janë krijuar dhe veprojnë.

Nga ana tjetër, linja e tretë e arsyetimit juridik, e shfaqur në praktikën gjyqësore të gjykatave të posaçme penale, arsyeton se formalisht ligji penal material mund dhe duhet të zbatohet ashtu sikurse tradicionalisht është zbatuar nga praktika gjyqësore e gjykatave të posaçme dhe ashtu sikurse është bekuar edhe nga Kolegji Penal i Gjykatës së Lartë ndër vite. Por kjo mënyrë e zbatimit të nenit 334 të Kodit Penal, e mbivendosur me dënimin e marrë sipas nenit 234/a, 284/a, 333 dhe 333/a të Kodit Penal, është e papranueshme dhe e papajtueshme me nenin 4, 7, 17, 34 dhe 135 të Kushtetutës. Kjo linjë arsyetimi konkludon se mbivendosja e sanksioneve të parashikuara në nenin 334 të Kodit Penal, në raport me sanksionet e marra si dënim për konsumimin e veprave penale formale dhe latente, cenon parimin *ne bis in idem* në kuptimin material. Pikërisht mbi bazën e këtij arsyetimi është iniciuar kontrolli kushtetues në Gjykatën Kushtetuese, me qëllim që të shfuqizohet neni 334 i Kodit Penal në pjesët e kontestuara.[59]

6. Argumentet kushtetuese kundër nenit 334 të Kodit Penal

i) *Cenimi i parimit të pavarësisë funksionale të pushtetit gjyqësor*

Fillimisht duhet të sillet në vëmendje se dispozita, shtesën fikse të dënimit me burgim apo me gjobë, e paracakton njëlloj qoftë për organizatorët, ekzekutorët, shtytësit dhe ndihmësit. Ndryshe nga sa parashikohet në paragrafin e dytë të nenit 27 të Kodit Penal, ku përgjegjësia penale shkallëzohet sipas meritës së rëndësisë, kontributit dhe rrezikshmërisë së bashkëpunëtorëve, në nenin 334 të Kodit Penal nuk njihet kjo logjikë ligjore e proporcionalitetit të mënyrës së përcaktimit të përgjegjësisë penale. Në të njëjtën kohë dispozita atribuon përgjegjësi penale të njëllojtë dhe automatike si për krijuesit, organizuesit, drejtuesit apo pjesëtarët e organizatës kriminale, organizatës terroriste dhe grupit të strukturuar kriminal, apo edhe për

59 Shih Vendimin "*Për pezullimin e gjykimit dhe dërgimin e çështjes në Gjykatën Kushtetuese*" nr. 33 Regjistri Themeltar, datë 17.12.2021 të Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit.

financuesit e organizatës terroriste.

Duhet të sillet në vëmendje se dënimet penale duhet të karakterizohen nga disa parime kushtetuese, sikurse janë parimi i drejtësisë, parimi i proporcionalitetit dhe parimi i individualizimit të dënimit penal, parime të cilat frymëzohen nga neni 17 i Kushtetutës dhe gjejnë konkretizim në nenin 47 dhe në parashikimet e tjera të posaçme të Kodit Penal. Gjykata Kushtetuese në elaborimin e këtyre parimeve të së drejtës penale dhe veçanërisht në sqarimin e parimit kushtetues të drejtësisë së caktimit të dënimit penal ka vlerësuar ligjvënësi në përcaktimin e veprave penale dhe llojit të dënimit ka fushë të gjerë veprimi, kjo liri është e kufizuar kur është fjala për vlerësimin e fajit si element i domosdoshëm i përgjegjësisë penale dhe në raport me shkallën e tij për caktimin e llojit dhe masës së dënimit konkret, pasi këto elemente janë të vlerësueshme vetëm nga gjykatat e zakonshme rast pas rasti.[60] Në thelb kjo pjesë e pushtetit shtetëror është njohur nga kushtetutat moderne si pushtet natyral i gjykatave dhe kjo trashëgimi etatiste bën pjesë në premisat kryesore të ekzistencës së shtetit të së drejtës.

Parimi i shtetit të së drejtës, ku mbështetet një shtet demokratik, nënkupton sundimin e ligjit dhe mënjanimin e arbitraritetit, me qëllim që të arrihet respektimi dhe garantimi i dinjitetit njerëzor, drejtësisë dhe sigurisë juridike dhe se disa nga elementet e shtetit të së drejtës janë: parimi i ndarjes së pushteteve, siguria juridike dhe respektimi i të drejtave dhe lirive themelore të njeriut.[61] Në këtë aspekt Gjykata Kushtetuese ka theksuar në jurisprudencën e saj se legjislacioni penal ka për detyrë të mbrojë vlera të rëndësishme, të tilla si pavarësinë e shtetit dhe tërësinë e tij territoriale, dinjitetin e njeriut, të drejtat dhe liritë e tij, rendin kushtetues, pronën etj. (*neni 1/b të KP-së*). Ai bazohet në parimet kushtetuese të shtetit të së drejtës, të barazisë përpara ligjit, të drejtësisë në caktimin e fajësisë dhe të dënimit, si dhe të humanizmit (*neni 1/c të KP-së*). Ky legjislacion është një tregues kuptimplotë për çdo vend, në kuptimin se sa ai është në gjendje të balancojë të drejtën e shtetit për të siguruar rendin publik e shoqëror, nga njëra anë, me të drejtat dhe liritë e individit, nga ana tjetër.[62]

Në këtë kuptim vlerësohet se në përcaktimin e dënimit penal për vepra të ndryshme penale, organi legjislativ nuk duhet të ketë parasysh vetëm parimin e parashikimit me ligj të dënimit dhe atë të sigurisë juridike, për t'u konsideruar sakaq se përfundoi detyrimi për respektimin e nenit 4, 29, 42

60 Shih Vendimin nr. 47, datë 27.06.2012 të Gjykatës Kushtetuese.

61 Shih Vendimin nr. 29, datë 31.05.2010 të Gjykatës Kushtetuese.

62 Shih Vendimin nr. 1, datë 12.01.2011 dhe Vendimin nr. 47, datë 27.06.2012 të Gjykatës Kushtetuese.

dhe 135 të Kushtetutës dhe nenit 7 të KEDNJ. Përkundrazi, ligjvënësi duhet të marrë parasysh detyrimisht mjaftueshëm edhe konceptin e drejtësisë në përcaktimin e fajit dhe vetë përgjegjësisë penale në kuadër të parimit të shtetit të së drejtës dhe nëpërmjet formulimit të sanksionit penal t'i mundësojë gjyqtarit dhënien e një gjykimi të drejtë dhe proporcional në raste konkrete. Koncepti i fajit apo përgjegjësisë penale dhe përcaktueshmëria e pasojave juridike janë në një marrëdhënie tensioni njëra me tjetrën, marrëdhënie kjo për të cilën duhet gjetur një balancë funksionale kushtetuese.[63]

Në këtë drejtim duhet të sillen në vëmendje se nevojat dhe pritshmëritë e kontrollit shoqërisë të realiteteve të ndryshme sociale duket sikur gjejnë "përkthim" në politikat penale të rendeve juridike të ndryshme sipas strategjive të ndërhyrjes ndëshkuese të karakterizuara nga instrumente me natyrë të ndryshme (ndëshkuese në kuptim të ngushtë, ndaluese apo mbikëqyrëse). Në këtë drejtim, vërehet se, nëse domosdoshmëria e sanksionit penal nuk vihet në diskutim, ajo që diskutohet, në rastin konkret, është "*strategjia e ndërhyrjes ndëshkuese*" nga ana e ligjvënësit për të përmbushur qëllimin e dënimit, funksionin parandalues të tij dhe atë riedukues, të cilat janë dhe funksionet themelore të legjislacionit penal. Për rrjedhojë duhet të sillet në vëmendje konsiderata jurisprudenciale e Gjykatës Kushtetuese mbi konkluzionin gjyqësor të individualizimit të dënimit penal, jurisprudencë kjo e cila ka vlerësuar se dënimi penal është rezultat i vlerësimit të rrezikshmërisë shoqërore të veprës penale, nga njëra anë, dhe shkallës së fajit të autorit të saj, nga ana tjetër.

Për rrjedhojë çmohet se, është i vërtetë fakt se përcaktimi i veprave penale dhe llojeve të dënimeve janë në diskrecion të ligjvënësit, por ndërkohë individualizimi dënimit në lloj dhe në masë, rast pas rasti, është në diskrecion të gjykatës, e cila duke shqyrtuar gjithë elementët juridikë të veprës penale, shkallën e fajit dhe pasojat e ardhura nga vepra penale, cakton llojin dhe masën e dënimit për autorët e veprave penale. Si rrjedhojë, njëlloj sikurse ka arsyetuar Gjykata Kushtetuese në raste të ngjashme[64], vlerësohet se përcaktimi paraprakisht nga ligjvënësi i dënimit penal fiks për një fakt penal, pa u dhënë mundësia ligjore e gjykatës për të kryer operacionin ligjor të individualizimit të dënimit sipas nenit 47 të Kodit Penal, ndërhyn në atributet ekskluzive të gjykatës lidhur me caktimin dhe individualizimin e dënimit penal.

Duhet të sillet në vëmendje se Gjykata Kushtetuese ka shfuqizuar

63 Shih Vendimin BVerfGE 105, 135 të Gjykatës Kushtetuese Gjermane.

64 Shih Vendimin nr. 47, datë 27.06.2012 të Gjykatës Kushtetuese.

paragrafin e dytë të shtuar në nenin 55 të Kodit Penal[65], me anën e së cilës ligjvënësi urdhëronte gjykatat që automatikisht të zbatonin bashkimin aritmetik të dënimeve në të gjitha rastet kur personat kryenin krime kundër jetës me dashje, me përdorimin pa leje të armëve luftarake dhe municionit. Gjykata Kushtetuese arriti në konkluzionin se në çdo rast bashkimi i dënimeve duhet të kryhet nga gjykata, duke u referuar në kriteret e nenit 47 të Kodit Penal[66] dhe se në ligji nuk mund të përcaktojë rregulla të ndryshme nga këto për të individualizuar dënimin. Gjykata Kushtetuese në këtë rast vlerësoi se, duke përcaktuar mënyrën e dhënies së dënimit përmes bashkimit aritmetik të dënimeve, ligjvënësi u ka hequr gjykatave të sistemit gjyqësor të drejtën të vlerësojnë pikërisht elementet e parashikuara në paragrafin e dytë të nenit 47 të Kodit Penal, të cilat janë jo vetëm përcaktuese në individualizimin e drejtë të dënimeve penale, por njëkohësisht janë edhe në kompetencën ekskluzive të gjyqësorit. Në vlerësimin e Gjykatës Kushtetuese ky rregullim ligjor përbën cenim të parimit të ndarjes së pushteteve dhe të pavarësisë funksionale të pushtetit gjyqësor, cenon parimin e ndarjes së pushteteve si dhe përbën kufizim të kompetencave në dhënien e drejtësisë.[67]

E njëjta çështje antikushtetuese e rregullimit ligjor shtrohet për zgjidhje edhe në këtë rast. Ligjvënësi ka parashikuar nga paragrafin e parë të nenit 334 të Kodit Penal një rrethanë cilësuese të veprave penale të kryera në kuadrin e bashkëpunimit të posaçëm për të cilën ka parashikuar se shtesa fike të dënimit me burgim dhe me gjobë. Në këtë rast ligjvënësi ka urdhëruar gjykatat e posaçme të bashkojnë aritmetikisht dënimet penale.

Në këtë kontekst konkludohet se ometimi i nenit 334 për të përcaktuar hapësirën diskrecionale të gjykatës për individualizimin e dënimit shtesë me burgim apo me gjobë, i heq gjykatës së posaçme të drejtën të vlerësojnë rast pas rasti elementet e parashikuara në paragrafin e dytë të nenit 27 dhe të nenit 47 të Kodit Penal, të cilat janë jo vetëm përcaktuese në individualizimin e drejtë të dënimeve penale, por njëkohësisht janë edhe në kompetencën ekskluzive të pushtetit gjyqësor. Në këtë mënyrë konkludohet se neni 334 i Kodit Penal në këtë pjesë ka cenuar parimin kushtetues të pavarësisë funksionale të pushtetit gjyqësor dhe bashkë me të edhe parimin e ndarjes së pushteteve, duke qenë se kufizohen kompetencat e pushtetit të gjyqësisë dhe dhënies së drejtësisë në përcaktimin e përgjegjësisë penale, në kundërshtim me nenin 4, 7, 42 dhe 135 të Kushtetutës.[68] Gjykata Kushtetuese në këtë pjesë, përballë

65 Shih nenin 9 të Ligjit nr. 144/2013, që ka ndryshuar nenin 55 të Kodit Penal.

66 Shih Vendimin nr. 9/2016 të Gjykatës Kushtetuese, paragrafi 23.

67 Shih Vendimin nr. 9/2016 të Gjykatës Kushtetuese, paragrafi 26 – 27.

68 Shih për analogji konkluzionet e arritura nga Gjykata Kushtetuese në Vendimin nr. 9, datë

iniciativës për kontroll incidental kushtetues të paragrafit të parë të nenit 334 të Kodit Penal, do të duhet të mbajë qëndrimin jurisprudencial të mbajtur në Vendimin nr. 9/2016, me të cilin ndër të tjera ka shfuqizuar paragrafin e dytë të nenit 55 të Kodit Penal.

ii) *Cenimi i parimit të proporcionalitetit*

Duhet të sillet në vëmendje se balanca mes së drejtës së kufizuar dhe interesit publik nuk është gjë tjetër veçse gjetja nga legjislatori e pikës së ekuilibrit midis së drejtës së shtetit për të siguruar rendin publik e shoqëror, nga njëra anë, dhe mbrojtjes së të drejtave dhe lirive të individit, nga ana tjetër. Për këtë arsye sanksionet penale, për shkak të kufizimeve që përcaktojnë në të drejtat dhe liritë themelore të njeriut, parashikohen vetëm për ato lloj veprimesh ose mosveprimesh, të cilat, në përputhje me parimin e proporcionalitetit, janë të krahasueshme për nga rëndësia me vlerat që mbrojnë. Është e vërtetë se është në diskrecionin e ligjvënësit vlerësimi i mjetit të zgjedhur për ndëshkimin e shkelësve të ligjit dhe qëllimin që kërkohet të arrihet, por kur është fjala për parashikimin e dispozitave penale dhe sanksioneve përkatëse si *"ultima ratio"*, ligjvënësi duhet të udhëhiqet nga parimet kushtetuese dhe funksionet që karakterizojnë dënimet penale.[69]

Gjithashtu duhet të mbahet parasysh edhe jurisprudenca e Gjykatës Kushtetuese të Republikës Federale të Gjermanisë për sa i përket parimit të proporcionalitetit dhe drejtësisë në caktimin e dënimit penal, jurisprudencë e cila ka theksuar se ky parim rrjedh nga vetë parimi i shtetit të së drejtës, në fakt nga vetë thelbi i të drejtave themelore, sidomos i lirisë personale, të cilat duhet të kufizohen nga pushteti shtetëror vetëm në atë masë sa të jetë e domosdoshme për mbrojtjen e interesit publik. Kjo jurisprudencë sjell në vëmendje se rëndësi të veçantë parimi i proporcionalitetit merr në fushën penale, sidomos në atë të parashikimit të dënimeve dhe ekzekutimit të tyre dhe mënyrën se si mbrohen të drejtat e njeriut, duke e vlerësuar sakaq të drejtën penale si një mjet të rëndësishëm të mbrojtjes së bazave të një bashkëjetese të rregulluar në shoqëri, megjithëse jo si mjetin kryesor të mbrojtjes publike, me gjithë karakterin e saj më të fuqishëm. Në këtë kuptim kjo jurisprudencë, duke pasur parasysh rëndësinë e mbrojtjes penale të shoqërisë dhe pasojat ligjore që sjell zbatimi i saj tek inidividi ka konkluduar se përdorimi i saj

---

26.02.2016, paragrafi 26 dhe 27, mbi antikushtetutshmërinë e nenit 55 të Kodit Penal, kontroll incidental kushtetues i nisur nga Gjykata e Apelit Vlorë.

69 Shih Vendimet nr. 12, datë 14.04.2010 dhe Vendimin nr. 47, datë 27.06.2012 të Gjykatës Kushtetuese.

duhet t'u nënshtrohet kërkesave të parimit të proporcionalitetit, duke u udhëhequr kurdoherë në individualizimin e dënimit penal nga një raport i drejtë dhe konkret i fajit mbi llojin dhe masën e dënimit dhe nga një raport i drejtë me rrezikshmërinë e veprës penale dhe pasojave të shkaktuara nga ajo.[70]

Nga ana tjetër nuk duhet të neglizhohet funksioni i dhe qëllimi i dënimeve penale në një shoqëri demokratike dhe parimet që duhet të udhëheqin ligjvënësin në parashikimin e dënimeve penale në ligj. Në lidhje me arsyen e ekzistencës së dënimit penal, Gjykata Kushtetuese është shprehur se ai përmbush dy funksione të ndryshme, të cilat mund të konsiderohen si edukative. Nga njëra anë, qëndron *funksioni i parandalimit të përgjithshëm* të veprave penale, pasi kërcënimi se shteti do të zbatojë sanksione penale sa herë që shtetasit do të kryejnë veprime të dënueshme nga legjislacioni penal, funksionon si një mënyrë për të dekurajuar dhe parandaluar cilindo shtetas që të ndërmarrë veprime që bien në kundërshtim me normat penale. Nga ana tjetër, qëndron *funksioni i parandalimit të posaçëm*, i cili lidhet drejtpërsëdrejti me autorin e veprës, pasi duke zbatuar sanksionin penal synohet riedukimi i tij, në mënyrë që pas kryerjes së dënimit të mos ndërmarrë në të ardhmen veprime kriminale.[71]

Në përputhje me frymën e Kushtetutës, Gjykata Kushtetuese ka vlerësuar në jurisprudencën e saj se sanksioni penal i çfarëdolloj natyre duhet të synojë vetëm riedukimin dhe më pas integrimin e të dënuarit në jetën shoqërore dhe se që të jetë i pranueshëm dënimi penal në aspektin kushtetues, në përputhje me nenin 17/1 të Kushtetutës, duhet të jetë i drejtë. Në këtë mënyrë, që të mund të ketë një proces riedukativ të suksesshëm, duhet që ndëshkimi penal të perceptohet nga autori i veprës si i drejtë dhe në përpjesëtim me veprën e kryer.[72] Në këtë kuadër, duke qenë se sanksionet penale lejojnë një ndërhyrje intensive tek të drejtat themelore të njeriut, Gjykata Kushtetuese ka konkluduar më parë e detyrimi i caktimit me ligj i dy sanksioneve penale kryesore për të njëjtën vepër penale, diametralisht të kundërta me njëra-tjetrën për nga qëllimet që ndjekin, nuk mund të pajtohet dhe të jetë në përpjesëtim me gjendjen që i ka diktuar, pasi ashpërsia e dënimeve penale të dhëna për të njëjtin fakt penal nuk është proporcionale në raport me rëndësinë e shkeljes

70 Shih Vendimet BVerfGE 19,342; BVerfGE 88,203; BVerfGE 45,187 të Gjykatës Kushtetuese të Republikës Federale të Gjermanisë.

71 Shih Vendimin nr. 19, datë 01.06.2011 dhe Venidmin nr. 47, datë 27.06.2012 të Gjykatës Kushtetuese.

72 Shih Vendimin nr. 19, datë 01.06.2011 të Gjykatës Kushtetuese.

konkrete dhe me pasojat e mundshme që mund të vijnë prej saj.[73]

Gjithashtu vlerësohet e nevojshme të sillet në vëmendje se eksperienca ka treguar që ashpërsimi jo proporcional i sanksioneve penale nuk ka pasur gjithmonë ndikim pozitiv ose ndikimi ka qenë i papërfillshëm në arritjen e qëllimeve të legjislacionit penal. Si pasojë, gjatë përcaktimit të dënimit, organi legjislativ nuk duhet të ketë parasysh vetëm parimin e parashikimit me ligj të dënimit. Ai duhet që nëpërmjet formulimit të sanksionit t'i mundësojë gjyqtarit dhënien e një gjykimi të drejtë dhe proporcional në raste konkrete, në përputhje me kërkesat e parimit të shtetit të së drejtës, sigurisë juridike dhe respektimit të të drejtave dhe lirive themelore të individit.[74]

Në rastin konkret duhet të sillet në vëmendje se dënimi që gjykata e posaçme shqipton sipas nenit 27 dhe neni 47 të Kodit Penal në vendimin e saj përfundimtar është konkretizimi i vlerësimit kompleks për sa i përket të gjitha rrethanave objektive dhe subjektive që janë provuar në gjykim lidhur me fajësinë, pasojat, rrezikshmërinë e veprës, rrezikshmërinë e autorit, rrethanat lehtësuese dhe rrethanat rënduese të provuara. Për rrjedhojë prezumohet kushtetutshmërisht dhe ligjshmërisht në çdo rast se një vendim i tillë gjyqësor, aq më tepër kur merr formë të prerë[75] dhe shndërrohet në gjë të gjykuar[76], se përgjegjësia penale e autorit është e konkretizuar pikërisht në llojin dhe masën e sanksionit të shqiptuar si dënim penal në vendimin gjyqësor. Mbi bazën e këtij prezumimi kushtetues dhe ligjor rendi juridik lejon dhe detyron të dënuarin të vuaj dënimin penal, duke i kufizuar atij proporcionalisht të liritë dhe drejtat kushtetuese dhe ligjore.

Legjislatori në rregullimin e paragrafit të parë të nenit 334 të Kodit Penal nuk merr parasysh asnjë rrethanë objektive apo subjektive. Përkundrazi është ligjvënësi ai që e cakton dhe e individualizon masën e dënimit me burgim dhe me gjobë për një subjekt që kryen vepër penale në kuadrin e organizatës kriminale, organizatës terroriste apo grupit të strukturuar kriminal. Në këtë kuptim konkludohet se kjo mënyrë e rregullimit ligjor të individualizimit të përgjegjësisë penale për autorin e veprës penale në kuadër të bashkëpunimit të posaçëm penal shkel parimin e proporcionalitetit, në kundërshtim me kërkesat e nenit 17 të Kushtetutës, duke ashpërsuar pasojat e dënimit penal të dhënë për të njëjtin fakt dhe duke mos gjetur një zgjidhje ligjore që të autorizojë gjykatën për të kryej operacionin ligjor të individualizimit të

73 Shih Vendimin nr. 47 datë 26.07.2012 të Gjykatës Kushtetuese.

74 Shih Vendimin nr.13, datë 29.05.1997; Vendimin nr.65, datë 10.12.1999; Vendimin nr.47, datë 27.06.2012 të Gjykatës Kushtetuese.

75 Shih nenin 462 të Kodit të Procedurës Penale.

76 Shih Vendimin Unifikues nr. 2/2014 të Kolegjeve të Bashkuara të Gjykatës së Lartë.

drejtë dhe proporcional të përgjegjësisë penale.

iii) *Cenimi i parimit ne bis in idem*

Neni 34 i Kushtetutës[77] ka garantuar këto që nuk mund të dënohet më shumë se një herë për të njëjtën vepër penale dhe as të gjykohet sërisht, me përjashtim të rasteve kur është vendosur rigjykimi i çështjes nga një gjykatë më e lartë, sipas mënyrës së parashikuar me ligj. Shkelja e parimit kushtetues të gjësë së gjykuar në procesin penal passjell dhunimin parimit *ne bis in idem* të sanksionuar nga neni 34 i Kushtetutës. Kjo dispozitë kushtetuese rregullon njëherazi edhe aspektin material dhe procedural të parimit *ne bis in idem*.

Duhet të sillet në vëmendje se ligjvënësi ndërhyri në titullin dhe përmbajtjen e nenit 7 të Kodit të Procedurës Penale në vitin 2017 pikërisht për të saktësuar konceptin juridik të "*idem*-it". Më përpara titulli i kësaj dispozite formulohej "*Ndalimi i gjykimit dy herë për të njëjtën vepër*" dhe në vitin 2017 u riformulua në "*Ndalimi i gjykimit dy herë për të njëjtin fakt*". Edhe në përmbajtje të kësaj dispozite u realizua i njëjti ndryshim i fjalës "*vepër*"[78] me fjalën "*fakt*"[79]. Në këtë mënyrë ligjvënësi përputhi me standardet ndërkombëtare konceptin juridik të "*idem*-it", i cili mundëson zbatimin e parimit *ne bis in idem* në kuptimin material dhe procedural sipas vizionit të parashikuar nga neni 34 i Kushtetutës.

Më tej ky parim njihet dhe bëhet i zbatueshëm drejtpërdrejtë nga gjykatat përmes realizimit të marrëdhënieve juridiksionale me jashtë. Fillimisht ky parim në dimensionin e tij njihet nga shkronja "ç" e nenit 491 të Kodit të Procedurës Penale[80]. Nën të njëjtin dimension të nenit 34 të Kushtetutës parimi *ne bis in idem* garantohet edhe nga shkronja "d" e nenit 514 të Kodit

77 Kjo dispozitë parashikon se:

"*Askush nuk mund të dënohet më shumë se një herë për të njëjtën vepër penale dhe as të gjykohet sërish, me përjashtim të rasteve kur është vendosur rigjykimi i çështjes nga një gjykatë më e lartë, sipas mënyrës së parashikuar me ligj.*"

78 Deri në vitin 2017 kjo dispozitë formulohej: "*1. Askush nuk mund të gjykohet rishtas për të njëjtën vepër penale, për të cilën është gjykuar me vendim të formë së prerë, me përjashtim të rasteve kur është vendosur rigjykimi i çështjes nga gjykata kompetente.*"

79 Nga viti 2017 kjo dispozitë formulohet: "1. Askush nuk mund të gjykohet rishtas për të njëjtin fakt penal, për të cilin është gjykuar me vendim të formë së prerë, me përjashtim të rasteve kur është vendosur rigjykimi i çështjes nga gjykata kompetente."

80 Kjo pjesë e dispozitës parashikon se: "*Nuk mund të jepet ekstradimi: ...ç) kur ka filluar procedimi ose është gjykuar në Shqipëri edhe pse vepra është kryer jashtë shtetit;*"

të Procedurës Penale[81]. Tek rregullimi i parë ligjor i sjellë në vëmendje legjislatori përdor fjalën "*vepër*" për të identifikuar konceptin "*idem*" dhe në rregullin e dytë përdor fjalën "*fakt*".

Parimi *ne bis in idem* në legjislacionin italian rregullohet nga neni 649 të Kodit të Procedurës Penale[82] nën titullin ndalimi i një gjykimi të dytë. Kjo normë parashikon se i pandehuri apo i dënuari me vendim apo me dekret penal përfundimtar dhe të parevokueshëm, nuk mund të procedohet sërisht për të njëjtin fakt, edhe sikur kualifikimi juridik i tij ndryshon sipas një titulli vepre penale, përveç kur disponohet për rifillimin e procedimit penal për shkak se del se personi i konkluduar i vdekur rezulton i gjallë (shih pikën 2 të nenit 69 të Kodit të Procedurës Penale[83]) apo përveç rasteve të rifillimit të procedimit penal pas vendimit të pushimit (shih pikën 2 të nenit 345 të Kodit të Procedurës Penale[84]). Në paragrafin e dytë të kësaj dispozite parashikohet se, nëse, pavarësisht këtij ndalimi, nis sërisht një procedim penal për të njëjtin fakt, atëherë gjykata në çdo fazë dhe shkallë procedimi vendos pushimin e çështjes, duke treguar pikërisht këtë shkak të pushimit të çështjes në diapozitivin e vendimit.

Gjykata Kushtetuese e Republikës së Italisë, përmes një gjykimi incidental kontrolli kushtetues të kësaj dispozite, ka konkluduar se ka deklaruar pakushtetutshmërinë e nenit 649 të Kodit të Procedurës Penale, në pjesën që përjashton zbatimin e kësaj norme në rastin kur fakti i njëjtë procedohet sërisht nën një titull tjetër juridik, vetëm për arsyen se mbi faktin historik penal ekziston mundësia e konkurrimit formal të titujve të ndryshëm të faktit juridik tipik.[85] Gjykata Kushtetuese e Republikës së Italisë ka konkluduar se për zbatimin e parimit *ne bis in idem* duhet të prevalojë konceptimi faktik i *idem*-it dhe jo konceptimi juridik i tij. Kjo do të thotë se në çdo rast për zbatimin e këtij parimi *idem*-i duhet të njëjtësohet me konceptimin e tij sipas faktit historik penal dhe jo sipas kualifikimit juridik të ndryshëm të tij.

---

81 Kjo pjesë e dispozitës parashikon se: "*1. Vendimi i gjykatës së huaj nuk mund të njohet kur:…d) fakti për të cilin është dhënë vendimi nuk parashikohet si vepër penale nga ligji shqiptar;*"

82 Shih në web: https://www.altalex.com/documents/news/2014/12/18/esecuzione-giudicato. Vizituar me datë 13.02.2022.

83 Shih në web: https://www.altalex.com/documents/news/2014/03/26/imputato. Vizituar me datë 12.02.2022.

84 Shih në web: https://www.altalex.com/documents/news/2014/01/15/attivita-a-iniziativa-della-polizia-giudiziaria. Vizituar me datë 12.02.2022.

85 Shih Vendimin nr. 200/2016 të Gjykatës Kushtetuese të Republikës së Italisë. Shih në web: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2016&numero=200. Vizituar me datë 13.02.2022.

Parimi *ne bis in idem* në legjislacionin italian rregullohet nga neni 649 të Kodit të Procedurës Penale[86] nën titullin ndalimi i një gjykimi të dytë. Kjo normë parashikon se i pandehuri apo i dënuari me vendim apo me dekret penal përfundimtar dhe të parevokueshëm, nuk mund të procedohet sërisht për të njëjtin fakt, edhe sikur kualifikimi juridik i tij të ndryshojë sipas një titulli vepre penale, përveç kur disponohet për rifillimin e procedimit penal për shkak se del se personi i konkluduar i vdekur rezulton i gjallë (shih pikën 2 të nenit 69 të Kodit të Procedurës Penale[87]) apo përveç rasteve të rifillimit të procedimit penal pas vendimit të pushimit (shih pikën 2 të nenit 345 të Kodit të Procedurës Penale[88]). Në paragrafin e dytë të kësaj dispozite parashikohet se, nëse, pavarësisht këtij ndalimi, nis sërisht një procedim penal për të njëjtin fakt, atëherë gjykata në çdo fazë dhe shkallë procedimi vendos pushimin e çështjes, duke treguar pikërisht këtë shkak të pushimit të çështjes në diapozitivin e vendimit. Kjo do të thotë se parimi *ne bis in idem* në kuptimin procedural dhe material krijon në çdo rast një prekluzion ligjor[89] për autoritetin shtetëror që të ushtrojë pushtetin ndëshkues dhe gjithashu edhe të mbivendosë apo të përsërisë procesin penal për të njëjtin fakt dhe kundër të njëjtit person.

Gjykata sjell në vëmendje se Gjykata Kushtetuese e Republikës së Italisë, përmes një gjykimi incidental kontrolli kushtetues të kësaj dispozite, ka marrë në shqyrtim kushtetutshmërinë e nenit 649 të Kodit të Procedurës Penale të interpretuar ngushtë në elementet e tij konstitutiv nga e drejta e gjallë. Gjykata *a quo* ka parashtruar në këtë rast se dyshimet mbi antikushtetutshmërinë e këtij rregullimi ligjor bien në pjesën ku jurisprudenca kombëtare ka identifikuar kritere objektive më të kufizuara se sa kriteret e elaboruara nga jurisprudenca e GJEDNJ mbi nenin 4 të Protokollit nr. 7 të KEDNJ. Gjykata *a quo* vlerësoi se për të identifikuar "*idem*-in" në çdo rast duhet të prevalojnë argumentat e njëjtësisë së faktit historik dhe natyror dhe jo argumentat interpretativ apo kualifikues juridik.

Gjykata Kushtetuese e Republikës së Italisë, pasi solli në vëmendje

86 Shih në web: https://www.altalex.com/documents/news/2014/12/18/esecuzione-giudicato. Vizituar me datë 13.02.2022.

87 Shih në web: https://www.altalex.com/documents/news/2014/03/26/imputato. Vizituar me datë 12.02.2022.

88 Shih në web: https://www.altalex.com/documents/news/2014/01/15/attivita-a-iniziativa-della-polizia-giudiziaria. Vizituar me datë 12.02.2022.

89 "*Commetario breve al Codice di Procedura Penale*", Terza Edizione, G. Cian, A. Trabucchi, Conso Illuminati, Grevi, Giuliani, Wolters Kluwer, Cedam, Breviaria Iuris, Milano, 2020, faqe 3155 dhe 3157.

mënyrën se si e drejta e gjallë kishte interpretuar elementet përbërës objektiv të "*idem*-it" në zbatimin praktik të nenit 649 të Kodit të Procedurës Penale, vendosi të deklarojë antikushtetutshmërinë e nenit 649 të Kodit të Procedurës Penale, në pjesën që përjashton zbatimin e kësaj norme në rastin kur fakti i njëjtë procedohet sërisht nën një titull tjetër juridik (*nomen juris*), vetëm për arsyen se mbi faktin historik penal ekziston mundësia e konkurimit formal të titujve të ndryshëm të faktit juridik tipik.[90] Gjykata Kushtetuese e Republikës së Italisë ka konkluduar se për zbatimin e parimit *ne bis in idem* duhet të prevalojë konceptimi faktik i *idem*-it dhe jo konceptimi juridik i tij. Kjo do të thotë se në çdo rast për zbatimin e këtij parimi *idem*-i duhet të njëjtësohet me konceptimin e tij sipas faktit historik penal dhe jo sipas kualifikimit juridik të ndryshëm të tij. Një qëndrim i tillë është pranuar edhe në doktrinën procedurale penale.[91]

Neni 649 i Kodit të Procedurës Penale të Republikës së Italisë është vendosur në Titullin I të Librit X me titull "*Gjëja e gjykuar*". Ndërkohë në nenin 648 të Kodit të Procedurës Penale të Republikës së Italisë parashikohen se si formësohet gjëja e gjykuar sipas këtij modeli ligjor procedural penal, duke u parashikuar se do të konsiderohen vendime gjë e gjykuar ato të cilat kanë ezauruar mjetet e zakonshnshme të ankimit apo ato ndaj të cilave nuk është ushtruar ankim brenda afateve ligjore. Duke pasur parasysh përjashtimin eksplicit të nenit 649 të këtij Kodi të Procedurës Penale, sjell në vëmendje se edhe në këtë model legjislacioni procedural penal nuk mundet të aktivizojë parimin *ne bis in idem* një vendim pushimi i akuzës apo çështjes penale që nuk përbën gjë të gjykuar (duke referuar si përjashtim në nenin 345 të Kodit të Procedurës Penale të Republikës së Italisë).[92]

Në aspektin material të rregullimit të partimit *ne bis in idem* neni 34 i Kushtetutës, nga mënyra e formulimit të saj, ngjan me nenin 103 pika 3 e Kushtetutës së Republikës Federale të Gjermanisë[93]. Jurisprudenca

90 Shih Vendimin nr. 200/2016 të Gjykatës Kushtetuese të Republikës së Italisë. Shih në web: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2016&numero=200. Vizituar me datë 13.02.2022.

91 "*Commetario breve al Codice di Procedura Penale*", Terza Edizione, G. Cian, A. Trabucchi, Conso Illuminati, Grevi, Giuliani, Wolters Kluwer, Cedam, Breviaria Iuris, Milano, 2020, faqe 3157, ku referohet Vincenzo Manzini "*Trattato di procedura penale e di ordinamento giudiziario*", faqe 589.

92 Shih për më tepër edhe "*Commetario breve al Codice di Procedura Penale*", Terza Edizione, G. Cian, A. Trabucchi, Conso Illuminati, Grevi, Giuliani, Wolters Kluwer, Cedam, Breviaria Iuris, Milano, 2020, faqe 3157.

93 Shih në web: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0570. Vizituar me datë 01.01.2022.

e Gjykatës Kushtetuese Federale të Gjermanisë i ka dhënë këtij parimi dimensionin material dhe procedural, duke interpretuar se kjo garanci kushtetuese mbron këdo të mos dënohet dy herë për të njëjtin fakt material dhe se të mos ushtrohet ndjekje penale më shumë se një herë për të njëjtin fakt penal.[94] Në këtë logjikë kushtetuese neni 52 dhe 53 i Kodit Penal të Republikës Federale të Gjermanisë ka rregulluar zbatimin e ligjit penal në rastet kur formalisht fakti penal mund të kualifikohet në më shumë se një vepër penale dhe për rrjedhojë formalisht duket se më shumë se një dënim kumulohet për t'u aplikuar ndaj të njëjtit fakt penal.[95] Këto dispozita kanë pamundësuar që i njëjti fakt penal të dënohet më shumë se një herë dhe se qëllimi i këtij rregullimi ligjor material ka qenë krijimi i identitetit juridik të veprës penale dhe kufizimi i zbatimit të së drejtës penale materiale. Normat ligjore që rregullojnë konkurrimin e veprave penale dhe dënimeve në këtë mënyrë kanë balancuar raportin e drejtë ndërmjet fajit dhe dënimit me qëllimin për të garantuar drejtësinë e dënimit penal.[96]

Ky parim nuk gjendet i sanksionuar në Kushtetutën e Republikës së Francës. Në këtë legjislacion parimi *ne bis in idem* sanksionohet në pikën 1 të nenit 368 të Kodit të Procedurës Penale[97], duke rregulluar vetëm dimensionin procedural të tij. Më tej në nenin 6 të këtij Kodi[98], nën të njëjtën logjikë dhe mënyrë të rregullimit ligjor, parashikohet se ekzistenca e një vendimi gjyqësor penal gjë të gjykuar dënimi apo pafajësie shuan ndjekjen penale dhe se ajo në këto kushte nuk mund të zhvillohet më.

Megjithatë, edhe pse në legjislacionin e këtij shteti nuk rregullohet në mënyrë eksplicite parimi *ne bis in idem* në dimensionin material, ka qenë Gjykata e Kasacionit dhe Këshilli Kushtetues që e kanë artikuluar jurisprudencialisht ekzistencën e këtij parimi. Këshilli Kushtetues i Republikës së Francës ka vlerësuar se rast pas rasti do të duhet që të analizohen katër elemente juridik përbërës të zbatimit të parimit *ne bis in idem*, konkretisht:

---

94 Shih Vendimin BVerfGE 12, 62, 66, datë 04.12.2007 – 2BvR 38/06 të Gjykatës Kushtetuese të Republikës Federale të Gjermanisë.

95 Shih "*Il principio del ne bis in idem*", Corte Constituzionale, Servizio studi, Area di diritto comparato, a cura di P. Passaglia, con contributi di C. Guerrero Pico, S. Pasetto, Z. T. Rorig, z. Torrisi, faqe 37.

96 Shih Vendimin datë 03.05.2012, StR 109/12, BGH të Republikës Federale të Gjermanisë.

97 Shih në web: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/. Vizituar me datë 01.01.2022.

98 Shih në web: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000024458637/#LEGISCTA000024458641. Vizituar me datë 01.01.2022.

1) *Identiteti juridik i faktit penal;*
2) *Identiteti juridik i objektit të mbrojtur nga norma penale;*
3) *Natyra e njëjtë e sanksioneve;*
4) *Identiteti juridik i organit gjykues.*

Sipas kësaj jurisprudence, mjafton një element që të mos përputhet që të mos ekzistojë ndalesa ligjore e parimit *ne bis in idem*.[99] Gjykata e Kasacionit ka konkluduar se mjafton që objekti i mbrojtur nga ligji penal të jetë i ndryshëm dhe në këtë rast normat penale dhe dënimet e ndryshme do të duhet të zbatohen edhe ndaj të njëjtit fakt.[100] Nga ana tjetër jurisprudenca e këtij institucioni ka konkluduar se parimi ne bis in idem në kuptimin e tij material dhunohet në rastet kur për të njëjtin fakt penal jepen dy dënime për vepra penale të kualifikuara sipas dispozitave të ndryshme.[101] Ndërkohë Këshilli Kushtetues e ka trajtuar parimin *ne bis in idem* në kuptimin material jo si një parim kushtetues i posaçëm por në funksionin e respektimit të parimit kushtetues të dënimit penal proporcional, të drejtë dhe të sigurisë juridike.[102]

Ndërkohë në Kushtetutën e Mbretësisë së Spanjës nuk parashikohet në mënyrë eksplicite parimi *ne bis in idem* dhe se në Projektin e Kushtetutës së vitit 1978 ky parim ishte sanksionuar në paragrafin e tretë të nenit 9. Megjithatë ky parim është zhvilluar nga jurisprudenca e Gjykatës Kushtetuese, duke interpretuar nenin 25 të Kushtetutës[103] dhe duke e bërë pjesë të parimeve kushtetuese.[104] Ky interpretim ka synuar që të kufizohet dhe të kontrollohet pushteti i shtetit për të ndëshkuar penalisht (*jus puniendi*)[105] dhe që ky pushtet të ushtrohet në mënyrë proporcionale.[106] Qëllimi i kësaj jurisprudence kushtetuese është shmangia e reagimit ndëshkues joproporcional apo eksesit

99 Shih Vendimin EADS, datë 18.03.2015, çështja "*M. John L. et autres*" të Këshillit Kushtetues të Republikës së Francës.

100 Shih Vendimin nr. 14-85.548, datë 08.12.2015 të Gjykatës së Kasacionit të Republikës së Francës.

101 Shih Vendimin nr. 15-80.732, datë 04.05.2016 të Gjykatës së Kasacionit të Republikës së Francës.

102 Shih Vendimin EADS, datë 18.03.2015, çështja "*M. John L. et autres*" të Këshillit Kushtetues të Republikës së Francës.

103 Shih në web: https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf. Vizituar me datë 01.01.2022.

104 Shih Vendimin nr. 77/1983, datë 03.10.1983 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

105 Shih Vendimin nr. 159/1985, datë 27.11.1985 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

106 Shih Vendimin nr. 154/1990, datë 15.10.1990, FJ 3; Vendimin nr. 177/1999, datë 11.10.1999, FJ 3 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

ndëshkimor të shtetit.[107]

Pikërisht për të përjashtuar mundësinë e dënimit dy herë të një fakti penal dhe për të garantuar respektimin e parimit kushtetues material *ne bis in idem* neni 8 i Kodit Penal të Mbretërisë së Spanjës[108] ka rregulluar mënyrën se si do të zbatohen normat penale nga gjykata rast pas rasti kur duket se disa kualifikime dhe dënimet formalisht konkurojnë. Parimi *ne bis in idem* në këtë jurisprudencë kushtetuese është vlerësuar i lidhur në mënyrë të pazgjidhshme me parimin e proporcionalitetit, parimin e sigurisë juridike dhe tipicitetit të veprave penale të parashikuara në ligj, parimin e mbrojtjes efektive të të drejtave themelore dhe parimin e gjë së gjykuar në procesin penal.[109] Gjykata Kushtetuese e Mbretërisë së Spanjës ka vlerësuar se mos respektimi i parimit *ne bis in idem* në kuptimin material cenon parancinë kushtetuese të parashikueshmërisë së sanksioneve dhe se në çdo rast shumatorja e dënimit të bashkuar kalon kufirin kushtetues të dënimit proporcional, duke imponuar sakaq një sanksion penal të paparashikuar nga ligji.

Gjykata Kushtetuese e Mbretërisë së Spanjës ka zhvilluar në jurisprudencën e saj teknikën e kontrollit të tre elementëve juridik për të konkluduar nëse ekziston rast pas rasti ndalesa materiale e parimit *ne bis in idem*. Elementet që duhet të analizohen në këto raste janë:

1) *Identiteti juridik i subjektit;*
2) *Identiteti juridik i faktit;*
3) *Identiteti juridik i objektit të mbrojtur nga ligji.*

Sipas kësaj jurisprudence është detyrë kushtetuese dhe ligjore më së pari e gjykatave të pushtetit gjyqësor që të kontrollojnë nëse ekzistojnë elementet juridik të aktivizimit të ndalesës materiale dhe procedurale të parimit *ne bis in idem*. Megjithatë, nëse kjo nuk ka ndodhur, atëherë të njëjtën analizë dhe shqyrtim duhet ta bëjë edhe Gjykata Kushtetuese përmes shqyrtimit të ankimit individual kushtetues (*amparo*).[110] Jurisprudenca e Gjykatës Kushtetuese të

107 Shih "*Il principio del ne bis in idem*", Corte Constituzionale, Servizio studi, Area di diritto comparato, a cura di P. Passaglia, con contributi di C. Guerrero Pico, S. Pasetto, Z. T. Rorig, z. Torrisi, faqe 73.

108 Shih në web: https://www.legislationline.org/download/id/6443/file/Spain_CC_am2013_en.pdf. Vizituar me datë 01.01.2022.

109 Shih Vendimin nr. 27/1981, datë 20.07.1981; Vendimin nr. 989/2011, datë 23.03.2012 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

110 Shih Vendimin nr. 48/2007, datë 12.03.2007, FJ 3; Vendimin nr. 91/2008, datë 21.07.2008, FJ 2; Vendimi nr. 91/2009, datë 20.04.2009, FJ 6; Vendimin nr. 69/2010, datë 18.10.2010 , FJ 3, Vendimin nr. 126/2011, datë 18.07. 2011, FJ 16 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

Mbretërisë së Spanjës ka konkluduar se në çdo rast kur objekti i veprave penale apo marrëdhënia juridike e mbrojtur është e ndryshme, atëherë nuk ka pengesë sipas parimit *ne bis in idem* për zbatimin e ligjit penal mbi të njëjtin fakt dhe se dhënia e më shumë se një dënimi është në përputhje me parimin e proporcionaitetit. Më tej, kur marrëdhënia juridike e cenuar nga fakti penal është i njëjtë atëherë parimi *ne bis in idem* në kuptimin material ndalon zbatimin më shumë se një herë të ligjit penal. Kjo do të thotë se që kushtetutshmërisht një fakt penal të dënohet më shumë se një herë nga ligji do të duhet që normat penale të cenuara të mbrojnë marrëdhënie juridike të ndryshme dhe se secila prej tyre të mbrojë vlera kushtetuese të ndryshme.[111] Kjo do të thotë se secili prej sanksioneve penale duhet të ndështkojë subjektin aktiv të veprës penale për cenimin e një marrëdhënie juridike të mbrojtur nga ligji.[112]

Parimi *ne bis in idem* është trajtuar edhe në jurisprudencën e Gjykatës Kushtetuese të Republikës së Shqipërisë. Sipas kësaj jurisprudence kushtetuese, ideja e parimit *ne bis in idem* nuk qëndron tek zbatimi dy a më shumë herë i të njëjtës normë penale, por te mosgjykimi e mosdënimi përsëri i subjektit për të njëjtën vepër penale, për të cilën ai është dënuar më parë me një vendim të formës së prerë nga një gjykatë e caktuar me ligj. Gjykata Kushtetuese ka vlerësuar se duhet të mbahet parasysh se kriteri "*e njëjta vepër*" i referohet të njëjtit veprim, sjellje, fakt, vepër penale dhe kualifikim ligjor të tyre, të cilat formojnë bazën e kësaj vepre dhe për të cilin personi është dënuar apo liruar. Nëse gjenden elementë të njëjtë, parimi *ne bis in idem* ndalon çdo dënim tjetër ose procedim të mëtejshëm.[113]

Interesant dhe me shumë vlerë mbetet trajtimi i parimit *ne bis in idem* dhe dimensioni material i nenit 34 të Kushtetutës në arsyetimin paralel të një vendimi të Gjykatës Kushtetuese.[114] Në këtë arsyetim paralel artikulohet se ndalimi kushtetues i dënimit më shumë se një herë për të njëjtën vepër penale është shprehje e parimit të së drejtës penale, se dënimi duhet të jetë i drejtë, që do të thotë se dënimi duhet të jetë në përputhje me natyrën dhe shkallën e rrezikshmërisë shoqërore të veprës penale, me rrethanat e kryerjes së veprës dhe personalitetin e të akuzuarit. Ky parim përjashton deklarimin fajtor dhe

111 Shih Vendimin nr. 234/1991, datë 10.12.1991 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

112 Shih Vendimin nr. 188/2005, datë 04.07.2005, FJ 5; Vendimin nr. 236/2007, datë 07.11.2007, FJ14 të Gjykatës Kushtetuese të Mbretërisë së Spanjës.

113 Shih Vendimin nr. 5, datë 08.03.2005; Vendimin nr. 10, datë 02.04.2009; Vendimin nr. 33, datë 22.07.2011 dhe Vendim nr. 8, datë 28.02.2012 të Gjykatës Kushtetuese.

114 Shih Vendimin nr. 41, datë 29.12.2005 të Gjykatës Kushtetuese. Shih "*Vendime të Gjykatës Kushtetuese të Republikës së Shqipërisë 2005*", Botim i Gjykatës Kushtetuese, Tiranë 206, faqe 358 – 361.

dënimin më shumë se një herë të të akuzuarit për të njëjtën vepër penale, për të cilën është dhënë një herë një vendim përfundimtar, apo cilësimin e të njëjtës vepër penale sipas dispozitave të ndryshme penale, kur cilësimi ligjor i veprës një herë bëhet sipas një ligji të përgjithshëm dhe një herë sipas një ligji të posaçëm, ose kur njëra dispozitë mund të quhet si nënseksion i një dispozite tjetër.

Sipas këtij qëndrimi, ndalimi kushtetues i parimit *ne bis in idem* në kuptimin material përjashton gjithashtu konsiderimin në të njëjtën kohë të një rrethane si rrethanë cilësuese dhe si rrethanë rënduese. Sipas të drejtës penale, një dënim i mëparshëm nuk mund të merret parasysh më tepër së një herë për qëllimet e përcaktimit të dënimit në rastet kur dënimi përbën një rrethanë rënduese të palidhur me cilësimin ligjor të veprës penale. Po kështu, një dënim i mëparshëm nuk mund të merret në konsideratë përsëri në rastin kur koncepti i "veprës penale të përsëritur" apo i "kryerjes së një vepre penale nga një person i cili ka kryer tashmë një vepër penale" përdoret si argument në mbështetje të dënimit (deklarimit fajtor). Në këtë qëndrim sillet në vëmendje se ka raste kur një sjellje (akt) kriminale, në pamje të parë, duket se përbën më tepër se një vepër penale, megjithëse një ekzaminim më i kujdesshëm tregon se duhet të procedohet vetëm një vepër penale sepse, kjo e fundit (vepra penale) përfshin të gjitha shkeljet që përfshihen në veprat e tjera. Për këtë qëllim jepet si shembull rasti kur sjellja (akti) kriminale, e cila përbën dy vepra penale, njëra prej të cilave përmban ekzakt të njëjtët elementë si tjetra plus edhe një tjetër. Për pasojë, kjo linjë arsyetimi paralel e gjyqtarëve të Gjykatës Kushtetuese thekson se duhet të ekzaminohet rast pas rasti nëse të tilla veprat penale kanë ose jo të njëjtët elementë të domosdoshëm për t'u konsideruar të njëjta faktikisht dhe juridikisht.[115]

115 Në rastin konkret tre gjyqtarët që kanë arsyetuar paralelisht kanë vijuar arsyetimin konkret se:

> "*Nga vendimet e gjykatave të zakonshme rezulton se kërkuesit janë deklaruar fajtorë dhe dënuar për veprat penale të "Organizimit dhe drejtimit të organizatës kriminale me qëllim trafikimin e narkotikëve", parashikuar nga neni 284/a/1 të Kodit Penal dhe atë të "Krijimit të bandë së armatosur dhe të organizatës kriminale", parashikuar nga neni 333 i Kodit Penal.*
>
> Për të konkluduar nëse kërkuesit janë dënuar më shumë se një herë për të njëjtën vepër, Gjykata duhet të verifikojë nëse këto vepra penale kanë të njëjtët elementë të domosdoshëm. Kështu, të dyja figurat e veprave penale që parashikojnë nenet 284/a/1 dhe 333 të Kodit Penal, parashikojnë krijimin dhe drejtimin e organizatave kriminale, por dallimi ndërmjet tyre qëndron në atë që organizata kriminale që parashikon dispozita e parë ka një qëllim të posaçëm - atë të "trafikimit të lëndëve narkotike", ndërsa organizata që parashikon dispozita tjetër, është e përgjithshme. Përveç kësaj, e njëjta veprimtari me qëllim trafikimin e narkotikëve që ka formuar anën objektive të veprës penale të parashikuar nga neni 284/a/1 i Kodit Penal, e cila është një sjellje e posaçme, përbën anën objektive të veprës penale të parashikuar nga neni 333 i Kodit Penal. Për pasojë, e

Zbatimin e ligjit penal sipas parimit kushtetues *ne bis in idem* në dimensionin material e ka trajtuar edhe Kolegji Penal dhe Kolegjet e Bashkuara të Gjykatës së Lartë. Në këtë jurisprudence është arsyetuar se ndalimi ligjor i dënimit më shumë se një herë për të njëjtën vepër penale është shprehje e parimit të së drejtës penale i cili përjashton jo vetëm deklarimin fajtor dhe dënimin e të gjykuarit më shumë se një herë për të njëjtën vepër penale, por edhe kualifikimin ligjor të së njëjtës vepër sipas dispozitave të ndryshme të Kodit Penal. Nuk mund të bëhet cilësimi ligjor i veprës një herë sipas një dispozite të përgjithshme dhe një herë sipas një dispozitë të posaçme.[116]

Kolegjet e Bashkuara të Gjykatës së Lartë kanë arsyetuar se në thelb i "njëjti fakt", është e njëjta shkelje, dhe cenohet vetëm njëherë e njëjta marrëdhënie juridike.[117] Më tej arsyetohet se konflikti i normave i përket fushës së zbatimit dhe cilësimit të ligjit dhe është i lidhur me zbatimin dhe interpretimin e përpiktë të ligjit penal material dhe se përcaktimi i saktë i normës që parashikon veprën penale, ka një rëndësi themelore, sepse është një parakusht për respektimin e parimit të ligjshmërisë, që një person të merret në përgjegjësi penale, e më pas ndaj tij të zbatohet sanksioni penal, sipas figurës së veprës penale saktësisht të kryer prej tij, kjo për shkak se është e ndaluar ndëshkimi i të njëjtit fakt që përbën vepër penale, më shumë se një herë. Kolegjet e Bashkuara të Gjykatës së Lartë kanë arsyetuar se një fakt penal duhet të dënohet vetëm një herë dhe do të duhet të zbatohet vetëm një normë penale sepse në të kundërt, do të cenohej parimi themelor i ndalimit të gjykimit dy herë për të njëjtën vepër penale (*ne bis in idem*).

Parimi i ndalimit të gjykimit dy herë për të njëjtën vepër penale përbën bazën themelore logjike dhe juridike të zbatimit të ligjit, në rastin kur kemi të bëjmë me praninë e një pluraliteti normash inkriminuese, të cilat në pamje të parë (*prima facie*) duken të gjitha si të zbatueshme, por që vetëm njëra prej tyre gjen zbatim. Kolegjet e Bashkuara vlerësojnë se ky parim zbatohet jo

---

njëjta sjellje, në të njëjtën kohë, është cilësuar edhe sipas një dispozite që parashikon një vepër të përgjithshme penale (neni 333 i Kodit Penal) edhe sipas një dispozite që parashikon një vepër të posaçme penale (neni 284/a/1 i po këtij Kodi), gjë që është e papranueshme. Këtu kemi parasysh edhe faktin se nuk është vërtetuar se në planin e veprimtarisë së tyre kriminale, kërkuesit kishin përfshirë edhe kryerjen e krimeve të tjera, përveç trafikimit të narkotikëve.

Për pasojë, mendojmë se kërkuesit janë dënuar më shumë se një herë për të njëjtën vepër penale, gjë që vjen në kundërshtim me nenin 34 të Kushtetutës."

116 Shih Vendimin Nr.56550-00998-00-2009 i Regj. Themeltar, Nr.00-2011-970 i Vendimit (68), datë 29.02.2012 të Kolegjit Penal të Gjykatës së Lartë.

117 Shih Vendimin Unifikues Penal nr. 3/2015 të Kolegjeve të Bashkuara të Gjykatës së Lartë, paragrafi 22.

vetëm në procedurën penale, por edhe në të drejtën penale materiale. Në bazë të këtij parimi, është i ndaluar procedimi dy herë i një personi për një fakt që përbën vepër penale, për të cilin është dhënë një vendim gjyqësor i formës së prerë që është bërë i pakundërshtueshëm. Gjithashtu, sipas këtij parimi, ndalohet për të njëjtin person edhe atribuimi i më shumë se një shkeljeje ligjore lidhur me të njëjtin fakt. Domethënë, vijojnë Kolegjet e Bashkuara të Gjykatës së Lartë, është i ndaluar për të njëjtin fakt atribuimi i më shumë se një shkeljeje të normës penale, kur shkelja e normës është e mjaftueshme, në raport me marrëdhënien juridike të cenuar dhe përmban elementet e veprës penale për caktimin e një dënimi penal në një masë proporcionale.[118]

Zbatimi i parimit të ndalimit të gjykimit më shumë se një herë për të njëjtën vepër në të drejtën penale materiale është i lidhur me funksionin e mbrojtjes së lirisë personale, parimin e sigurisë juridike dhe me atë të ligjshmërisë në të drejtën penale.

Ky parim gjen edhe rregullim ndërkombëtar normativ. Kështu pika 7 e nenit 14 të Paktit Ndërkombëtar për të Drejtat Civile dhe Politike ka rregulluar parimin *ne bis in idem* në apektin procedural.[119] Ky rregullim ligjor i jep përparësi më së shumti kualifikimit ligjor të veprës penale në ligjin e brendshëm të çdo shteti në mënyrë që të vlerësohet nëse jemi para të njëjtit "*idem*" apo vepre penale. Në këtë mënyrë prevalon më shumë rregullimi dhe emërtimi formal i faktit penal se sa kualifikimi material i identitetit të faktit për të cilin individi është dënuar.

Parimi *ne bis in idem* rregullohet edhe nga Statuti i Romës në nenin 20.[120] Ndryshe nga rregullimi i mëlartëm, Statuti i Romës "*idem-in*" e përshkruan si sjellje të individit, që do të thotë se nuk kërkon analizën formale të kualifikimit juridik të veprës penale por kërkon analizën materiale të sjelljes që ka përbërë anën objektive të veprës penale objekt procedimi.

Parimi *ne bis in idem* rregullohet edhe nga neni 53 i Konventës Europiane për Vlefshmërinë e Gjykimeve Penale. Në pikën 1 të kësaj dispozite Konventa përdor termin "*për të njëjtin fakt*" për të përshkruar "*idem-in*".[121]

---

118 Shih Vendimin Unifikues Penal nr. 3/2015 të Kolegjeve të Bashkuara të Gjykatës së Lartë, paragrafi 23 – 26.

119 Shih në web: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Vizituar me datë 01.01.2022.

120 Shih në web: https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf. Vizituar me datë 01.01.2022.

121 Shih Ligjin nr. 9068, datë 15.5.2003, "*Për ratifikimin e "Konventës Europiane për Vlefshmërinë Ndërkombëtare të Gjykimeve Penale*". Ndër të tjera pika 1 e kësaj dispozite parashikon se:

Gjithashtu ky parim gjen rregullim juridik ndërkombëtar edhe në Konventën Europiane për Transferimin e Procedimeve Penale.[122] Pika 1 e nenit 35 të këtij akti ndërkombëtar e rregullon njëlloj konceptin juridik të "*idem*-it", duke përdorur konceptin "*për të njëjtin akt*".[123]

Parimi *ne bis in idem* është rregulluar edhe në nenin 54 të Marrëveshjes së Schengen-it[124]. Gjithashtu dhe në mënyrë të ngjashme me dispozitën e KEDNJ, neni 50 i Kartës së të Drejtave Themelore të Bashkimit Europian[125] ka sanksionuar parimin *ne bis in idem*. Në Marrëveshjen e Schengen-it dallohet se "*idem-i*" përshkruhet me termin akt (*acts*), që nënkupton veprime apo mosveprime të anës objektive të veprës penale.[126] Kjo mënyrë formulimi

---

"*1. Një person, ndaj te cilit është zhvilluar një gjykim penal evropian, nuk mund te procedohet, gjykohet apo te behet objekt ekzekutimi i një sanksioni ne një shtet tjetër pale për te njëjtin fakt kur:*

a) ai është shpallur i pafajshëm;

b) sanksioni i vendosur:

i) është ekzekutuar plotësisht ose është duke u ekzekutuar;

ii) është objekt i një faljeje ose amnistie ne tërësinë e tij ose për pjesën e paekzekutuar;

iii) nuk mund te ekzekutohet me, pasi është parashkruar;

c) gjykata konstaton fajësinë e autorit, por nuk vendos ndonjë sanksion."

122 Ligji nr. 8497, datë 10.6.1999 "*Për ratifikimin e Konventës së Këshillit të Europës "Për transferimin e procedimeve në çështjet penale*".

Shih në web: https://www.crca.al/sites/default/files/publications/Permledhese%20e%20akteve%20nderkombetare%20per%20Drejtesine.pdf. Vizituar me datë 08.01.2021.

123 Në nenin 35 me titull "*Ne bis in idem*" parashikohet ndër të tjera se:

"*1. Një person, në lidhje me të cilën është dhënë një vendim gjyqësor penal përfundimtar dhe i detyrueshëm, për të njëjtin akt, mund të mos ndiqet penalisht, dënohet ose t'i nënshtrohet një sanksioni në një shtet tjetër kontraktues:*

(a) në qoftë se ai është falur;

(b) në qoftë se sanksioni i kërkuar për t'u zbatuar:

(i) ka qenë zbatuar plotësisht ose është duke u zbatuar, ose

(ii) i është nënshtruar faljes ose amnistisë, plotësisht, ose në lidhje me pjesën e pazbatuar, ose

(iii) nuk mund të zbatohet për shkak të kalimit të afatit kohor;

c) në qoftë se gjyqi e ka shpallur fajtor të pandehurin pa kërkuar zbatimin e një sanksioni."

124 Shih Marrëveshjen Schengen datë 14 Qershor 1985 të realizuar ndërmjet shteteve të Benelux-it, Republikës Federale të Gjermanisë, Republikës së Francës mbi heqjen graduale të kontrollit dhe kufijve të përbashkët, 22.09.2000, OJ L 239/19.

125 Akt i shpallur solemnisht nga Parlamenti Europian, Këshilli dhe Komisioni në Strasburg me datë 12.12.2007, OJ 14.12.2007, C 303/1.

126 Shih për më tepër analizën e bërë në çështjen "*Leopold Henri Van Esbroeck*", Case C-436/04, Vendim i GJEDNJ datë 9 Mars 2006.

në këtë marrëveshje ka qenë e qëllimtë, për të mos bërë pengesë për lirinë e lëvizjes së individëve faktin e mungesës së hanomizimit të ligjeve shteteve palë kontraktore dhe në mënyrë që të garantohet siguria juridike e kujtdo individi që nuk do të përndiqet, gjykohet apo dënohet për së dyti për të njëjtat veprime apo mosveprime.[127] Ndërkohë në nenin 50 të Kartës së të Drejtave Themelore përdoret termi vepër penale (*offence*), duke i dhënë më shumë shkas interpretimit formal të konceptit "*idem*".

GJED në jurisprudencën e saj e ka njohur në disa vendime parimin *ne bis in idem* si parim themelor të së drejtës komunitare.[128] Kjo jurisprudencë merr parasysh se identifikimi i ndalesës që vjen nga parimi *ne bis in idem* arrihet nga analiza e tre elementeve, duke i individualizuar ato si vijon:

1) *Identiteti i fakteve;*
2) *Njëjtësia e subjektit aktiv të faktit;*
3) *Njëjtësia e marrëdhënies juridike të mbrojtur nga e drejta*.[129]

GJED, në mënyrë që të identifikohet njëjtësia e konceptit "*idem*" ka vlerësuar se në çdo rast duhet të vlerësohet ekzistenca e një tërësie rrethanash të cilat janë pazgjidhshmërisht të lidhura me njëra-tjetrën.[130] Në mënyrë që të vlerësohet nëse faktet materiale janë të njëjta GJED ka theksuar se duhet të mbahet parasysh përshkrimi faktik i tyre dhe lidhja që ato kanë në kohë, në hapësirë dhe për nga subjekti që i ka kryer dhe se nga kjo analizë duhet të konkludohet se e gjithë tërësia e veprimeve dhe e mosveprimeve përbëjnë një fakt të vetëm të kundraligjshëm dhe sit ë tillë të pandashëm. GJED ka vlerësuar se vetëm fakti i ekzistencës së një qëllimi unik kriminal nga ana e autorit që lidh fakte të caktuara nuk përbën detyrimisht lidhje objektive të tyre, në rastet kur konstatohet se nuk ekziston lidhja materiale e kërkuar e tyre në kohë dhe në hapësirë. Duke pasur parasysh këto konsiderata jurisprudenciale, GJED ka vlerësuar se kriteri relevant për identifikimin e "*idem-it*" do të jetë rast pas rasti identiteti i veprimeve apo mosveprimeve

127 Shih çështjen C-385/01 "*Gözütok and Brügge*", Vendim i GJED [[2003] ECR I-1345], paragrafi 33.

128 Shih çështjen "*Limburgse Vinyl Maatschappij NV (LVM) and Others v. Commission of the European Communities*", Joined Cases C-238/99 P, C-244/99 P, C-245/99 P, C-247/99 P, C-250/99 P to C-252/99 P and C-254/99 P, § 59, Vendim i GJED datë 15 Tetor 2002.

129 Shih çështjen "*Aalborg Portland A/S and Others v. Commission of the European Communities*", Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, § 338, Vendim i GJED datë 7 Janar 2004.

130 Shih çështjen "*Norma Kraaijenbrink*", Case C-367/05, Vendim i GJED datë 18 Korrik 2007; çështja Case C-467/04 "*Gasparini and Others*", [2006] ECR I-9199, Vendim i GJEDN, paragraph 54; çështjen Case C-150/05 "*Van Straaten*", [2006] ECR I-9327, Vendim i GJED, paragraph 48.

material dhe bashkëekzistenca e një tërësie faktesh të lidhura në mënyrë të pazgjidhshme, pavarësisht nga kualifikimi formal ligjor i tyre në ligjet e shteteve të ndryshme apo interest që kërkohet të mbrohet nga ligji.

Edhe Konventa Americane mbi të Drejtat e Njeriut e ka rregulluar parimin *ne bis in idem*. Ky parim rregullohet në nenin 8 të saj, duke përdorur si terminologji për të përshkruar "*idem-in*" fjalën "*shkak*" (*cause*). Këtë dallim në terimonoligjinë e përdorur nga ky akt ndërkombëtar në raport Paktin Ndërkonbëtar për të Drejtat Civile dhe Politike me ka përdorur edhe Gjykata Ndër-Americane për të Drejtat e Njeriut për theksuar se duhet të mbahet një kriter interpretativ më i zgjeruar dhe më material për sa i përket konceptit "*idem*" dhe qëduhet të shkojë në favor të mbrojtjes së lirisë dhe sigurisë së individit.[131]

Të njëjtin rregullim ka bërë edhe neni 4 i Protokollit 7 të KEDNJ[132]. Vihet re se në mënyrën se si është formuluar kjo dispozitë për të përshkruar "*idem-in*" përdoren koncepti formal i veprës penale (*offence*), gjë që në dukje jep përshtypjen se privilegjon interpretimin formal të kualifikimit ligjor të faktit penal në legjislacionin e çdo shteti. Megjithatë GJEDNJ në jurisprudencën e saj e ka zhvilluar parimin *ne bis in idem* edhe me aspektin e tij material[133], duke e ridimesionuar edhe konceptin e "*idem-it*" në drejtim të analizës së elementeve material karakterizues së sjelljes së dënueshme nga ligji. GJEDNJ, duke mbajtur parasysh të gjithë dallimet në terminologji të akteve të ndryshme ndërkombëtare që sanksionojnë parimin ne bis in idem dhe gjithashtu edhe qëndrimet jurisprudenciale të gjykatave simotra, ka konkluduar se për zbatimin e nenit 4 të Protokollit nr. 7 të KEDNJ, pavarësisht kualifikimit të ndryshëm të faktit nga ligjet e shteteve palë kontraktore, do të duhet të mbahet parasysh rast pas rasti tërësinë te rrethanave të faktit që i atribuohen të njëjtit autor, të cilat janë të lidhura me njëra-tjetrën në mënyrë të pazgjidhshme në kohë dhe në hapësirë, ekzistenca e të cilave duhet të provohet në mënyrë që të sigurohet një dënim apo të procedohet penalisht.[134]

131 Shih çështjen "*Loayza-Tamayo v. Peru*", Vendim datë 17 Shtator 1997, Series C No. 33, paragrafi 66, i Gjykatës Ndër-Amerikane për të Drejtat e Njeriut.

132 Shih në web: https://www.echr.coe.int/Documents/Guide_Art_4_Protocol_7_ENG.pdf. Vizituar me datë 01.01.2022.

133 Shih për shembull çështjen "*Kapetanios et autres c. Greece*", Ap. Nr. 3453/12; Nr. 42941/12; Nr. 9028/13, Vendim datë 30.04.2015 i GJEDNJ. Në këtë vendim GJEDNJ, pasi ka konkluduar mbi natyrën autonome të veprës penale sipas jurisprudencës së saj, ka konkluduar se dënimet e njëjta penale dhe administrative të dhëna për të njëjtin fakt cenojnë garancinë e parashikuar nga neni 4 i Protokollit nr. 7 të KEDNJ.

134 Shih çështjen "*Sergey Zolotukhin v. Russia*", Application no. 14939/03, Vendim i Dhomës së Madhe të GJEDNJ datë 10.02.2009, paragrafi 84.

Në rastin konkret rezulton se neni 334 i Kodit Penal parashikon dënim penal të shtuar për bashkëpunëtorët në veprat penale të kryera në kuadrin e organizatës kriminale, organizatës terroriste dhe grupit të strukturuar kriminal. *Ratio* e dënimit penal të shtuar është vetëm fakti që veprat penale kryhen në kuadër të këtyre formave të posaçme të bashkëpunimit penal. Thënë ndryshe, vetëm kjo rrethanë cilësuese dhe rënduese njëkohësisht e veprës penale të kryer e shton dënimin penal për veprën me pesë vjet burgim apo me një të tretën e dënimit me gjobë të caktuar.

Nga ana tjetër dhe në të njëjtën kohë secili prej këtyre subjekteve drejtues, organizatorë, krijues, financues apo pjesëmarrës të organizatës kriminale, organizatës terroriste apo grupit të strukturuar kriminal kanë konsumuar veprat penale të parashikuara nga neni 234/a, neni 234/b, neni 284/a, neni 333 apo neni 333/a i Kodit Penal. Duhet të sillet në vëmendje se këto dispozita e parashikojnë si vepër penale formale dhe latente krijimin, organizimin, drejtimin, financimin dhe pjesëmarrjen në organizatën kriminale, organizatën terroriste, bandën e armatosur dhe grupin e strukturuar kriminal, duke përcaktuar si dënime masa që nisin nga 2 vjet burgim e përfundojnë deri në 30 vjet burgim. Edhe në këtë rast ligjvënësi dënon penalisht me burgim bashkëpunimin e posaçëm dhe mjafton ky fakt për të merituar dënime nga 2 deri në 30 vjet burgim.

Në këto raste identiteti juridik dhe faktik i faktit penal është i njëjtë, qoftë në nenin 234/a, 284/a, 333 dhe 333/a në raport me nenin 334 të Kodit Penal. Konkretisht fakti penal në bazën e të dy hipotezave ligjore është bashkëpunimi i posaçëm në formën e organizatës kriminale, organizatës terroriste apo grupit të strukturuar kriminal. Në këto raste identiteti juridik i objektit që mbrojnë këto dispozita është identik. Objekti parësor i këtyre veprave penale është siguria publike e cila kanoset seriozisht nga format e paligjshme të organizimit kolektiv të individëve dhe nga ana tjetër garantimin e së drejtës së individëve për t'u organizuar kolektivisht vetëm për qëllime të ligjshme.[135] Në këto raste identiteti juridik i sanksioneve penale që këto dispozita parashikojnë është i njëjtë, konkretisht dënimi me burgim. Ajo që ndryshon është vetëm masa e dënimit me burgim. Në këto raste identiteti juridik i organit shtetëror është i njëjti, konkretisht gjykatat e posaçme penale, sipas nenit 135 të Kushtetutës.

Në të njëjtën mënyrë konkludohet në këto raste edhe mbi analizën juridike që propozon jurisprudenca e Gjykatës Kushtetuese të Mbretërisë së Spanjës mbi identifikimin e parimit *ne bis in idem*.

135 Shih nenin 9, 46 dhe 47 të Kushtetutës.

Nga ana tjetër rezulton se edhe analiza juridike që realizojnë gjykatat ndërkombëtare të sjella në vëmendje më lart mundëson arritjen e të njëjtit konkluzion. Në këto raste bashkëpunimi i posaçëm penal në formën e organizatës kriminale, organizatës terroriste dhe grupit të strukturuar kriminal, i shtrirë në kohë dhe në hapësirë dhe nën të cilin kryhet vepra penale shërben si shkak ligjor për të ndëshkuar dy herë penalisht të njëjtën sjellje humane të kundraligjshme.

Nga e gjithë kjo analizë konkludohet se Kodi Penal në mbivendosjen e dënimeve sipas nenit 234/a me nenin 334, sipas nenit 284/a me neni 334, sipas nenit 333 me nenin 334 dhe sipas nenit 333/a me nenin 334 të Kodit Penal ka parashikuar dy dënime penale për të njëjtin fakt penal, konkretisht bashkëpunimin e posaçëm në formën e organizatës kriminale, organizatës terroriste apo grupit të strukturuar kriminal. Në këto raste, sipas çdo analize që propozojnë secili prej kritereve të identifikuar nga institucionet kombëtare dhe ndërkombëtare të drejtësisë sikurse u sollën në vëmendje më lart mbi konceptin juridik "*idem*", konkludohet se këto dispozita penale *de facto* dhe *de jure* dënojnë të njëjtat veprime të autorëve bashkëpunëtorë. Për rrjedhojë konkludohet se në të gjitha rastet e bashkëpunimit të posaçëm penal në Shqipëri, kur kryhen vepra penale në kuadrin e organizatës kriminale, organizatës terroriste apo grupit të strukturar kriminal, i autori fajtor dënohet për së dyti për të njëjtin fakt penal, krejt ndryshe nga sa ka parashikuar neni 34 i Kushtetutës dhe krejt ndryshe nga sa kërkon parimi *ne bis in idem* që të disiplinohet pushteti ndëshkimor penal shtetëror (*jus puniendi*).

Konstatohet se në relacionet bashkëshoqëruese të Kodit Penal apo të ndryshimeve ligjore penale ndër vite të nenit 334 të Kodit Penal, që janë paraqitur në Kuvend, nuk ka asnjë shpjegim eksplicit se pse bashkëpunimi i posaçëm penal dënohet penalisht dy herë, konkretisht një herë në nenin 234/a, 234/b, 284/a, 333 dhe 333/a dhe një herë në nenin 334 të Kodit Penal. Në këto kushte, njëlloj sikurse analiza që ka përdorur në mënyrë analoge Gjykata Kushtetuese[136], konkludohet se ka paqartësi dhe spontanitet në qëllimin e përzgjedhjes së mjetit të ashpërsimit të dënimit penal dhe në dënimin e dyfishtë të bashkëpunimit të posaçëm që bën neni 334 i Kodit Penal. Sakaq konkludohet se cenohet parimi kushtetues i sigurisë juridike përmes cenimit të parimit *ne bis in idem* në kuptimin material, në kundërshtim me nenin 4, 29 dhe 34 të Kushtetutës.

136 Shih Vendimin nr. 9, datë 26.02.2016 të Gjykatës Kushtetuese.

7. Vlerësimi i Gjykatës Kushtetuese

Gjykata Kushtetuese vendosi që këtë kontroll kushtetues incidental të ligjit ta kalojë për gjykim në Mbledhjen e Gjyqtarëve. Pas shqyrtimit të kërkesës, Mbledhja e Gjyqtarëve në Gjykatën Kushtetuese vendosi moskalimin e çështjes për shqyrtim në seancë plenare.[137]

Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese, lidhur me argumentet për cenimin e parimit të drejtësisë në caktimin e dënimit penal, pasi solli në vëmendje nenin 47 dhe pikën 5 të nenit 28 të Kodit Penal, vlerësoi se, kur pjesëtari i organizatës kriminale ose i grupit të strukturuar kriminal kryen vepër penale, ai dënohet sipas dispozitave penale përkatëse të veprës së kryer, duke i shtuar këtij dënimi edhe 5 vjet burgim. Mbledhja e Gjyqtarëve vlerësoi se në këtë kuptim, duke iu referuar rastit konkret neni 334 i Kodit Penal shton me 5 vjet dënimin e parashikuar nga neni 298, pika 3, të Kodit Penal, i cili nuk përbën dënim fiks, për shkak të formës së organizimit si grup i strukturuar kriminal. Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese vlerësoi se Kodi Penal parashikon për gjyqtarin mundësinë e individualizimit të dënimit për veprën penale të kryer ndaj dhe, shtimi i dënimit me 5 vjet i parashikuar nga ky nen nuk cenon thelbin e së drejtës të gjykatës në individualizimin e dënimit për veprën konkrete penale të kryer. Sakaq Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese vlerësoi se argumentet e parashtruara në kontrollin incidental kushtetues të nenit 334 të Kodit Penal janë haptazi të pabazuara.

Lidhur me pretendimin për cenimin e parimit kushtetues *ne bis in idem* dhe atë të sigurisë juridike, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese ka arsyetuar se, kur i pandehuri kryen vepër penale në rrethanën cilësuese të bashkëpunimit në formën e krimit të organizuar, si në rastin konkret atë të "*Ndihmës për kalim të paligjshëm të kufirit*" në bashkëpunim në formën e pjesëmarrjes në grup të strukturuar kriminal, dënimi i tij, sipas parashikimeve të neneve 298 dhe 334 të Kodit Penal, nuk cenon parimin *ne bis in idem*. Në këto lloj rastesh, zbatimi i nenit 334 të Kodit Penal shton masën e dënimit të parashikuar nga ligji për veprën penale të kryer për shkak të rrethanës cilësuese së pjesëmarrjes në krim të organizuar. Në këtë kuptim, neni 334 i Kodit Penal nuk zbatohet veçmas dhe nuk është autonom, por ai shoqëron atë dispozitë penale të veprës konkrete penale të kryer dhe e cilëson veprën penale si të kryer nga organizata kriminale ose grupi i strukturuar kriminal. Për sa më sipër, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese vlerëson se ky pretendim i gjykatës referuese është haptazi i pabazuar, pasi

137 Shih Vendimin e Mbledhjes së Gjyqtarëve të Gjykatës Kushtetuese nr. 42, datë 05.04.2022.

gjykata referuese e ka lidhur cenimin e këtij parimi me atë të *ne bis in idem* në kuptimin material dhe për sa kohë që ajo e gjen të pabazuar këtë të fundit, e vlerëson të pabazuar edhe pretendimin për cenimin e parimit të sigurisë juridike.

Lidhur me argumentet për cenimit të parimit të proporcionalitetit në mënyrën se si paragrafi i parë dhe i dytë i nenit 334 të Kodit Penal përcaktojnë masën e dënimit fiks për secilion nga bashkëpunëtorët pavarësisht llojit dhe rolit të tyre, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese vlerësoi se gjykata referuese e ka mbështetur pretendimin e saj për cenimin e parimit të proporcionalitet vetëm duke referuar në standardet e elaboruara në jurisprudencën kushtetuese, por nuk ka arritur të evidentojë të drejtën ose lirinë kushtetuese konkrete, e cila është kufizuar në kundërshtim me kriteret e nenit 17 të Kushtetutës. Për rrjedhojë, argumentet e gjykatës referuese janë haptazi të pabazuara.

Lidhur me argumentet për cenimin e nenit 18 të Kushtetutës në pjesën ku ligjvënësi nuk ka trajtuar në mënyrë të barabartë përgjegjësinë penale të shtuar të pjesëmarrësve të bandës së armatosur sikurse ka rregulluar përgjegjësinë penale të shtuar të pjesëmarrësve të organizatës kriminale ose grupit të strukturuar kriminal, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese ka vlerësuar se përcaktimi i politikave penale është një fushë me kompetencë ekskluzive e ligjvënësit dhe se në rastin konkret ndodhemi para kategorive të individëve që janë në kushte objektivisht të ndryshme, pasi dispozitat e referuara nga gjykata referuese parashikojnë dhe zbatohen për kategori të ndryshme të veprave penale të dënueshme penalisht. Për rrjedhojë, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese ka vlerësuar se nuk ka arritur të identifikojë të drejtën themelore kushtetuese ose atë ligjore e cila gëzon mbrojtje nga neni 18 i Kushtetutës, ndaj ai është haptazi i pabazuar.

Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese në përfundim ka vlerësuar se pretendimet e parashtruara nga gjykata referuese në lidhje me papajtueshmërinë e dispozitës ligjore të kundërshtuar me Kushtetutën janë haptazi të pabazuara, pasi ajo nuk ka arritur të arsyetojë nga pikëpamja e kushtetutshmërisë se në ç`mënyrë shprehja "*duke i shtuar dënimit për veprën penale të kryer edhe pesë vjet burgim*" në pikën 1 të nenit 334 të Kodit Penal e pengon atë në përcaktimin e përgjegjësisë penale dhe në individualizimin e dënimit penal, pra nuk ka arritur të plotësojë kriterin e dytë të legjitimimit, atë të parashtrimit të arsyeve serioze për antikushtetutshmërinë e dispozitës së kundërshtuar referuar në normat dhe parimet konkrete të Kushtetutës.

Lidhur me kërkimin e gjykatës referuese për shfuqizimin e pikës 2 të nenit 334 të Kodit Penal, Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese ka vlerësuar se këto parashikime nuk janë të zbatueshme në çështjen konkrete dhe se për rrjedhojë gjykatës referuese i mungon lidhja e drejtpërdrejtë mes çështjes së kushtetutshmërisë dhe zgjidhjes së çështjes konkrete në shqyrtim para saj, duke konkluduar sakaq në mosmarrjen në shqyrtim të këtij rregullimi penal material.

8. Refleksione mbi vendimin e Gjykatës Kushtetuese

Vlerësoj se vendimi i sjellë në vëmendje më lart është një shembull i shmangies së Gjykatës Kushtetuese nga detyrimi kushtetues për të dhënë drejtësi kushtetuese. Në të gjithë argumentet të lidhura drejtpërdrejtë me vlerësimin e rastit, në një apo e shumta në dy fjali, dhënia ne drejtësisë kushtetuese shmanget përmes konsideratës klishe të bërë rutinë tashmë nga kjo gjykatë, konkretisht se pretendimet e gjykatës referuese janë haptazi të pabazuara dhe nuk sjellin argumente serioze antikushtetutshmërie. Duket sikur me këtë togfjalësh kjo gjykatë është e gatshme dhe e aftë të rrëzojë gjithçka i vjen për të shqyrtuar.

I vetmi moment ku Gjykata Kushtetuese është përpjekur të analizojë në themel është pretendimi për cenimin e parimit kushtetues *ne bis in idem* dhe parimin e sigurisë juridike. Në këtë pjesë të analizës vlerësoj se me qëllim dhe me keqbesim Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese del tej argumenteve kushtetuese të parashtruara nga gjykata referuese dhe objektin e mosmarrëveshjes kushtetuese në gjykim e formëson vetë pavarësisht se çfarë është elaboruar në vendimin e ndërmjetëm përmes të cilit është iniciuar kontrolli kushtetues incidental i ligjit. Kështu gjykata referuese ka argumentuar se parimi kushtetues ne bis in idem dhe parimi i sigurisë juridike cenohet nga penalizmi material dy herë i rrethanës së bashkëpunimit të posaçëm, konkretisht në nenin 234/a, nenin 234/b, 333 dhe 333/a në raport me nenin 334 të Kodit Penal. Ndërkohë Mbledhja e Gjyqtarëve të Gjykatës Kushtetuese konkludon se nuk ka cenim të parimit kushtetues *ne bis in idem* dhe të parimit të sigurisë juridike nga parashikimi i nenit 298 të Kodit Penal nga njëra anë dhe penalizmit të bashkëpunimit të posaçëm të nenit 334 të Kodit Penal.

Në këtë mënyrë Mbledhja e Gjykatës Kushtetuese vendosi të mos i shqyrtojë problematikat thelbësore kushtetuese që mbart në vetvete prej vitesh formulimi dhe parashikimi i nenit 334 të Kodit Penal. Në këto kushte mbetet detyrë e gjykatave të posaçme penale që të zgjidhin secilën prej këtyre

çështjeve kushtetuese penale përmes zhvillimit të praktikës gjyqësore.

9. Propozim për një interpretim ligjor ndryshe mbi problematikën e paragrafit të parë të nenit 334 të Kodit Penal

Kumti i jurisprudencës së Gjykatën Kushtetuese në Vendimin nr. 9/2016, mbi mënyrën se si duhet të realizohet operacioni i bashkimit të dënimeve penale të ndryshme nga ana e gjykatës, ishte se neni 55 i Kodit Penal duhet të zbatohet mbi kriteret e parashikuar nga neni 47 i tij. Vlerësoj se, nëse nuk gjendet një zgjidhje nga Gjykata Kushtetuese mbi këtë kontest kushtetues që është ngritur nga Gjykata e Posaçme e Apelit kundër Krimit të Organizuar dhe Korrupsionit, atëherë problematikën kushtetuese të respektimit të parimit të proporcionalitetit, të drejtësisë në caktimin dhe individualizimin e dënimit penal, të respektimit të pavarësisë funksionale të pushtetit gjyqësor do të duhet ta realizojnë gjykatat e posaçme apo Gjykata e Lartë përmes praktikës gjyqësore dhe jurisprudencës evolutive të tyre.

Lidhur me këtë problematikë vlerësoj se ekziston një zgjidhje ligjore interpretative pajtuese me Kushtetutën e paragrafit të parë të nenit 334 të Kodit Penal. Sigurisht që në aspektin formal të interpretimit të normës apo edhe teleologjik të saj kjo zgjidhje është shumë e sforcuar. Megjithatë kjo mënyrë e interpretimit të paragrafit të parë të nenit 334 të Kodit Penal do të respektojë parimet kushtetuese të individualizuara më lart si të cenuara nga zbatimi i kësaj pjese të dispozitës ligjore sikurse është shkruar dhe është dashur të vendoset nga ana e ligjvënësit.

Vlerësoj se shtesa fikse e dënimit me burgim prej 5 vitesh apo shtesa fikse prej 1/3 e dënimit me gjobë, që parashikohet në paragrafin e parë të nenit 334 të Kodit Penal, nuk duhet të shtohet në çdo rast automatikisht dhe aritmetikisht nga ana e gjykatave të posaçme mbi dënimin e individualizuar për veprën penale të kryer. Kjo mënyrë interpretimi pajtuese e togfjalëshit normativ "*duke i shtuar*" synon që shtesën fikse të dënimit ta realizojë përmes operacionit ligjor të bashkimit të dënimeve, sikurse Kodi Penal parashikon në nenin 55[138].

138 Kjo dispozitë e titulluar "*Caktimi i dënimeve për disa vepra penale*" parashikon se: "Kur veprimet ose mosveprimet përmbajnë elementet e disa veprave penale, si dhe kur personi ka kryer disa vepra penale për të cilat nuk është dhënë akoma vendim, gjykata më parë cakton dënimin për çdo vepër penale dhe në përfundim jep një dënim të vetëm, që përbëhet nga dënimi më i rëndë i shtuar.

Dënimi më i rëndë i shtuar nuk mund të kapërcejë shumën e përgjithshme të dënimeve të caktuara veç e veç, as kufirin më të lartë të parashikuar për llojin e dënimit të dhënë.

Në këtë mënyrë vlerësoj se, diskrecioni i munguar gjyqësor në caktimin e dënimit në paragrafin e parë të nenit 334 të Kodit Penal, ofrohet dhe kompensohet ligjërisht prej zbatimit në të këtë rast të nenit 55 sipas kritereve të parashikuara në nenin 47 të Kodit Penal. Në këtë mënyrë vlerësoj se gjykatat e posaçme ndreqin kushtetutshmërinë e munguar të paragrafit të parë të nenit 334 të Kodit Penal përmes operacionit të interpretimit pajtues me Kushtetutën të ligjit, duke realizuar sakaq edhe drejtësi kushtetuese në individualizimin e përgjegjësisë penale për bashkëpunëtorët në një nga format e posaçme të bashkëpunimit penal.

10. **Konkluzioni**

Për rrjedhojë të gjithçka u analizua dhe u arsyetua më lart arrij në konkluzionin se neni 334 i Kodit Penal dënon për së dyti të njëjtën sjellje të paligjshme të çdo pjesëmarrësi në organizatën kriminale apo në grupin strukturuar kriminal, konkretisht kryerjen e veprës penale në një nga këto forma të posaçme të bashkëpunimit. Për rrjedhojë në çdo rast që zbatohet neni 334 i Kodit Penal dënohet për të dytën herë individi bashkëpunëtor që ka marrë dënim sipas nenit 234/a, 284/a, 284/a, 333 apo 333/a të Kodit Penal. Për rrjedhojë në çdo rast të zbatimit të tij neni 334 i Kodit Penal dhunon parimin *ne bis in idem* në kuptimin material të parashikuar nga neni 34 i Kushtetutës.

Për sa më lart u arsyetua, arrihet në konkluzionin se Gjykata Kushtetuese duhet të shfuqizojë paragrafin e parë të nenit 334 të Kodit Penal, në pjesën që parashikon "*duke i shtuar dënimit për veprën penale të kryer edhe pesë vjet burgim, si dhe gjobën në masën një të tretën*", pasi vjen në kundërshtim me nenin 7, 17, 135/1 dhe 145/1 të Kushtetutës, pasi cenon parimin e ndarjes së pushteteve, parimin e proporcionalitetit, parimin e pavarësisë së pushtetit gjyqësor, si dhe përbën kufizim të juridiksionit dhe kompetencave të pushtetit gjyqësor në dhënien e drejtësisë. Ky konkluzion vlen edhe nëse Gjykata Kushtetuese do të konkludojë se ndërmjet nenit 334 të Kodit Penal nga njëra anë dhe nenit 234/a, 284/a, 333 dhe 333/a të Kodit Penal nga ana tjetër mund të realizohet gjyqësisht interpretimi pajtues dhe se këto norma penale nuk konkurojnë me njëra tjetrën.

Kur gjykata çmon se kryerja e shumë veprave penale nuk tregon rrezikshmëri të madhe të fajtorit, mund të japë si dënim përfundimtar dënimin më të rëndë që ka caktuar për një nga veprat penale.

Gjykata në vendimin përfundimtar jep një ose më shumë nga dënimet plotësuese të dhëna më vete për çdo vepër të veçantë."

Për sa më lart u arsyetua, arrihet në konkluzionin se Gjykata Kushtetuese duhet të shfuqizojë paragrafin e parë dhe të dytë të nenit 334 të Kodit Penal pasi vjen në kundërshtim me nenin 7, 17, 34, 135/1 dhe 145/1 të Kushtetutës, pasi cenon parimin e ndarjes së pushteteve, parimin e proporcionalitetit, parimin e pavarësisë së pushtetit gjyqësor si dhe përbën kufizim të juridiksionit dhe kompetencave të pushtetit gjyqësor në dhënien e drejtësisë dhe cenon parimin *ne bis in idem* në kuptimin kushtetues material të tij. Ky konkluzion vlen nëse Gjykata Kushtetuese do të vlerësojë se ndërmjet nenit 334 të Kodit Penal nga njëra anë dhe nenit 234/a, 284/a, 333 dhe 333/a të Kodit Penal nga ana tjetër nuk mund të realizohet gjyqësisht interpretimi pajtues dhe se këto norma penale konkurojnë me njëra tjetrën.

Nëse asnjë nga këto konkluzione nuk ndodhin të bëhen realitet në çështjen që po gjykohet në Gjykatën Kushtetuese, atëherë mbetet që gjykatat e posaçme apo Gjykata e Lartë të realizojë një interpretim pajtues të këtyre dispozitave ligjore. Interpretimi pajtues që mundet të garantojë respektimin e parimit *ne bis in idem* është ai, sipas të cilit nuk mundet të zbatohen njëherazi edhe neni 334 edhe nenet 234/a, 284/a, 333 dhe 333/a të Kodit Penal. Në këtë mënyrë do të duhet të konkludohet se veprat penale formale dhe latente të parashikuara nga neni 234/a, 284/a, 333 dhe 333/a të Kodit Penal do të kualifikohen dhe do të zbatohen si norma vetëm për sa kohë forma e posaçme e bashkëpunimit penal nuk ka kryer vepra penale të tjera. Në momentin kur forma e posaçme e bashkëpunimit ka kryer vepër tjetër penale, atëherë nuk do të zbatohen më nenet 234/a, 284/a, 333 dhe 333/a të Kodit Penal, pasi këto vepra penale do të trupëzohen juridikisht dhe do të përthithen nga neni 334 i Kodit Penal. Kjo mënyrë e zbatimit të ligjit penal do të ishte formalisht e paligjshme por përmes saj do të arrihej të zbatohej neni 34 i Kushtetutës.

Nga ana tjetër vlerësoj se shtesa e dënimit fiks prej 5 vitesh burgim apo 1/3 e gjobës së dhënë, mbi dënimin e individualizuar sipas veprës penale respektive të kryer, nuk do të duhet detyrimisht që të shtohet automatikisht dhe aritmetikisht nga ana e gjykatës. Përkundrazi, gjykata e posaçme në këto raste do të duhet të realizojë operacionin ligjor të bashkimit të dënimeve sipas nenit 55 të Kodit Penal. Duke sjellë në vëmendje jurisprudencën e Gjykatës Kushtetuese mbi zbatimin e nenit 55 të Kodit Penal përmes kritereve të parashikuara në nenin 47 të tij[139], gjykata e posaçme duhet të realizojë bashkimin e dënimit të individualizuar për veprën penale përkatëse të kryer me dënimin shtesë prej 5 vitesh burgim apo dënimin shtesë prej 1/3 e gjobës, të caktuar sipas nenit 334 të Kodit Penal. Në çdo rast të tillë do të

139 Shih Vendimin nr. 9/2016 të Gjykatës Kushtetuese.

jetë gjykata e posaçme, sipas kritereve të parashikuara në nenin 55 dhe 47 të Kodit Penal, që do të duhet të përcaktojë mënyrën ligjore se si këto dënime penale duhet të bashkohen me njëri tjetrin dhe se sa duhet të jetë dënimi i bashkuar përfundimisht për të pandehurin. Ky interpretim ligjor pajtues me Kushtetutën i paragrafit të parë të nenit 334 të Kodit Penal formalisht është nuk është i drejtë por përmes tij arrihet të garantohet zbatimi i nenit 4, 7, 17, 135 dhe 145 të Kushtetutës.

Bibliografia

E drejta pozitive

1. Kushtetuta;
2. KEDNJ dhe Protokollet Shtesë;
3. Marrëveshja Schengen datë 14 Qershor 1985 të realizuar ndërmjet shteteve të Benelux-it, Republikës Federale të Gjermanisë, Republikës së Francës mbi heqjen graduale të kontrollit dhe kufijve të përbashkët, 22.09.2000, OJ L 239/19;
4. Pakti Ndërkombëtar për të Drejtat Civile dhe Politike;
5. Kodi Penal;
6. Kodi i Procedurës Penale;
7. Karta e të Drejtave Themelore e Bashkimit Europian 12.12.2007, OJ 14.12.2007, C 303/1;
8. Ligji nr. 1470, datë 23.05.1952 botuar në Gazetën Zyrtare nr. 15/1952;
9. Ligji nr. 5591, datë 15.06.1977, të ndryshuar me Ligjin nr. 6300, datë 27.03.1981;
10. Ligji nr. 8279, datë 15.01.1998 "*Për disa ndryshime e shtesa në ligjin nr. 7895, datë 27.01.1995 "Për Kodin Penal të Republikës së Shqipërisë*";
11. Ligji nr. 8733, datë 24.01.2001 "*Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.01.1995, "Kodi Penal i Republikës së Shqipërisë*";
12. Ligji nr. 8920, datë 11.7.2002 "*Për ratifikimin e "Konventës së Kombeve të Bashkuara Kundër Krimit të Organizuar Ndërkombëtar" dhe dy Protokolleve shtesë të saj*";
13. Ligji Nr. 9275, datë 16.9.2004 "*Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë*", i

ndryshuar;

14. Ligji nr. 9686, datë 26.2.2007 "*Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar*;
15. Ligji nr. 9068, datë 15.5.2003, "*Për ratifikimin e "Konventës Europiane për Vlefshmërinë Ndërkombëtare të Gjykimeve Penale*";
16. Ligji nr. 8497, datë 10.6.1999 "*Për ratifikimin e Konventës së Këshillit të Europës "Për transferimin e procedimeve në çështjet penale*";
17. Ligji nr. 144/2013;
18. Kodi Penal i Republikës Federale të Gjermanisë;
19. Kodi Penal i Mbretërisë së Spanjës;
20. Kodi Penal i Republikës së Italisë;
21. Kodi Procedurës Penale i Republikës së Francës;
22. Dekreti i Presidentit të Republikës së Italisë nr. 309, datë 09.10.1990;

Jurisprudencë

1. Vendimi "*Për pezullimin e gjykimit dhe dërgimin e çështjes në Gjykatën Kushtetuese*" nr. 33 Regjistri Themeltar, datë 17.12.2021 i Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit;
2. Vendimi Nr. 59000-01410-00-2012 i Regjistri Themeltar, Nr. 00-2014-1935 i Vendimit (175), datë 16.07.2014 i Kolegjit Penal të Gjykatës së Lartë;
3. Vendimi nr. 14, datë 17.04.2007 të Gjykatës Kushtetuese;
4. Vendimi nr. 30791, datë 17.07.2013 të Seksionit VI Penal të Gjykatës së Kasacionit të Republikës së Italisë;
5. Vendimi nr. 19198, datë 21.04.2017 të Seksionit Penal III të Gjykatës së Kasacionit të Republikës së Italisë;
6. Vendimi nr. 42635, datë 03.11.2004 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë;
7. Vendimi nr. 7187, datë 19.02.2004 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;
8. Vendimi nr. 44369, datë 24.10.2014 të Seksionit Penal V dhe Vendimin

nr. 49995, datë 31.10.2017 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

9. Vendimi nr. 45388, datë 07.12.2005 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë;
10. Vendimi nr. 10.12.1990 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë;
11. Vendimi datë 27.02.1989 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë;
12. Vendimi nr. 2651, datë 21.01.2015 të Seksionit Penal V; Vendimin nr. 10380, datë 08.03.2019 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë;
13. Vendimi datë 07.12.1979 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë;
14. Vendimi nr. 17265, datë 24.04.2008 të Seksionit Penal I të Gjykatës së Kasacionit të Republikës së Italisë;
15. Vendimi nr. 10380, datë 08.03.2019 të Seksionit Penal V të Gjykatës së Kasacionit të Republikës së Italisë;
16. Vendimi nr. Datë 07.04.1989 të Seksionit Penal I dhe Vendimin nr. 4294, datë 29.01.2015 të Seksionit Penal VI i Gjykatës së Kasacionit të Republikës së Italisë;
17. Vendimi nr. 135, datë 03.12.2015 i Gjykatës së Shkallës së Parë për Krimet e Rënda;
18. Vendimi nr. 1, datë 16.01.2012 i Gjykatës së Shkallës së Parë për Krimet e Rënda;
19. Vendimi nr. 10, datë 10.02.2016 i Gjykatës së Apelit për Krimet e Rënda;
20. Vendimi nr. 20, datë 25.03.2011 i Gjykatës së Apelit për Krimet e Rënda;
21. Vendimi nr. 45, datë 02.07.2012 i Gjykatës së Apelit për Krimet e Rënda;
22. Vendimi Nr. 56550-00591-00-2016 Regjistri Themeltar, Nr. 00-2017-8 i Vendimit (3), datë 01.02.2017 i Kolegjit Penal i Gjykatës së Lartë;
23. Vendimi nr. 135, datë 03.12.2015 i Gjykatës së Shkallës së Parë për Krimet e Rënda;

24. Vendimi nr. 47, datë 27.06.2012 i Gjykatës Kushtetuese;
25. Vendimi nr. 29, datë 31.05.2010 i Gjykatës Kushtetuese;
26. Vendimi nr. 1, datë 12.01.2011 i Gjykatës Kushtetuese;
27. Vendimi nr. 47, datë 27.06.2012 i Gjykatës Kushtetuese;
28. Vendimi BVerfGE 105, 135 i Gjykatës Kushtetuese të Republikës Federale të Gjermanisë;
29. Vendimi nr. 9, datë 26.02.2016 i Gjykatës Kushtetuese;
30. Vendimet nr. 12, datë 14.04.2010 i Gjykatës Kushtetuese;
31. Vendimi BVerfGE 19, 342 i Gjykatës Kushtetuese të Republikës Federale të Gjermanisë;
32. Vendimi BVerfGE 88,203 i Gjykatës Kushtetuese të Republikës Federale të Gjermanisë;
33. Vendimi BVerfGE 45,187 i Gjykatës Kushtetuese të Republikës Federale të Gjermanisë;
34. Vendimi nr. 19, datë 01.06.2011 i Gjykatës Kushtetuese;
35. Vendimi nr. 13, datë 29.05.1997 i Gjykatës Kushtetuese;
36. Vendimi nr. 65, datë 10.12.1999 i Gjykatës Kushtetuese;
37. Vendimi Unifikues nr. 2/2014 i Kolegjeve të Bashkuara të Gjykatës së Lartë;
38. Vendimi BVerfGE 12, 62, 66, datë 04.12.2007 – 2BvR 38/06 i Gjykatës Kushtetuese të Republikës Federale të Gjermanisë;
39. Vendimi datë 03.05.2012, StR 109/12, BGH i Republikës Federale të Gjermanisë;
40. Vendimi EADS, datë 18.03.2015, çështja "*M. John L. et autres*" i Këshillit Kushtetues të Republikës së Francës;
41. Vendimi nr. 14-85.548, datë 08.12.2015 i Gjykatës së Kasacionit të Republikës së Francës;
42. Vendimi nr. 15-80.732, datë 04.05.2016 i Gjykatës së Kasacionit të Republikës së Francës;
43. Vendimi EADS, datë 18.03.2015, çështja "*M. John L. et autres*" i Këshillit Kushtetues të Republikës së Francës;
44. Vendimi nr. 77/1983, datë 03.10.1983 i Gjykatës Kushtetuese të

Mbretërisë së Spanjës;

45. Vendimi nr. 159/1985, datë 27.11.1985 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
46. Vendimi nr. 154/1990, datë 15.10.1990, FJ 3 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
47. Vendimi nr. 177/1999, datë 11.10.1999, FJ 3 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
48. Vendimi nr. 27/1981, datë 20.07.1981 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
49. Vendimi nr. 989/2011, datë 23.03.2012 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
50. Vendimi nr. 48/2007, datë 12.03.2007, FJ 3 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
51. Vendimin nr. 91/2008, datë 21.07.2008, FJ 2 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
52. Vendimi nr. 91/2009, datë 20.04.2009, FJ 6 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
53. Vendimi nr. 69/2010, datë 18.10.2010, FJ 3 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
54. Vendimi nr. 126/2011, datë 18.07. 2011, FJ 16 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
55. Vendimi nr. 234/1991, datë 10.12.1991 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
56. Vendimin nr. 188/2005, datë 04.07.2005, FJ 5 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
57. Vendimi nr. 236/2007, datë 07.11.2007, FJ14 i Gjykatës Kushtetuese të Mbretërisë së Spanjës;
58. Vendimi nr. 5, datë 08.03.2005 i Gjykatës Kushtetuese;
59. Vendimi nr. 10, datë 02.04.2009 i Gjykatës Kushtetuese;
60. Vendimi nr. 33, datë 22.07.2011 i Gjykatës Kushtetuese;
61. Vendimi nr. 8, datë 28.02.2012 i Gjykatës Kushtetuese;
62. Vendimi nr. 41, datë 29.12.2005 i Gjykatës Kushtetuese;

63. Çështja "*Leopold Henri Van Esbroeck*", Case C-436/04, Vendim i GJEDNJ datë 9 Mars 2006;

64. Çështja C-385/01 "*Gözütok and Brügge*", Vendim i GJED [[2003] ECR I-1345];

65. Çështja "*Limburgse Vinyl Maatschappij NV (LVM) and Others v. Commission of the European Communities*", Joined Cases C-238/99 P, C-244/99 P, C-245/99 P, C-247/99 P, C-250/99 P to C-252/99 P and C-254/99 P, § 59, Vendim i GJED datë 15 Tetor 2002;

66. Çështja "*Aalborg Portland A/S and Others v. Commission of the European Communities*", Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, § 338, Vendim i GJED datë 7 Janar 2004;

67. Çështja "*Norma Kraaijenbrink*", Case C-367/05, Vendim i GJED datë 18 Korrik 2007;

68. Çështja Case C-467/04 "*Gasparini and Others*", [2006] ECR I-9199, Vendim i GJEDN;

69. Çështja Case C-150/05 "*Van Straaten*", [2006] ECR I-9327, Vendim i GJED;

70. Çështja "*Loayza-Tamayo v. Peru*", Vendim datë 17 Shtator 1997, Series C No. 33, paragrafi 66, i Gjykatës Ndër-Amerikane për të Drejtat e Njeriut;

71. Çështja "*Kapetanios et autres c. Greece*", Ap. Nr. 3453/12; Nr. 42941/12; Nr. 9028/13, Vendim datë 30.04.2015 i GJEDNJ;

72. Çështja "*Sergey Zolotukhin v. Russia*", Application no. 14939/03, Vendim i Dhomës së Madhe të GJEDNJ datë 10.02.2009;

73. Vendimi nr. 45, datë 14.06.2021 i Gjykatës së Posaçme të Shkallës së Parë Kundër Krimit të Organizuar dhe Korrupsionit;

74. Vendimi nr. 39, datë 25.05.2012 i Gjykatës së Shkallës së Parë për Krimet e Rënda;

75. Vendimi nr. 75, datë 06.12.2012 i Gjykatës së Apelit për Krimet e Rënda;

76. Vendimi nr. 50, datë 29.07.2008 i Gjykatës së Shkallës së Parë për Krimet e Rënda;

77. Vendimi nr. Nr. 59000-00240-00-2013 Regj. Themeltar, Nr. 00-2015-

585 i Vendimit (38), datë 11.03.2015 i Kolegjit Penal të Gjykatës së Lartë;

78. Vendimi nr. 36, datë 26.09.2009 i Gjykatës së Apelit për Krimet e Rënda;
79. Vendimi nr. 11, datë 16.02.2009 i Gjykatës së Shkallës së Parë për Krimet e Rënda;
80. Vendimi Nr. 56550-00582-00-2009 i Regj. Themeltar, Nr.00-2010-283 i Vendimit (22), datë 20.01.2010 i Kolegjit Penal të Gjykatës së Lartë;
81. Vendimi nr. 57, datë 13.10.2009 i Gjykatës së Apelit për Krimet e Rënda;
82. Vendini nr. 43, datë 13.07.2009 i Gjykatës së Shkallës së Parë për Krimet e Rënda;
83. Vendimi nr. 61, datë 24.12.2010 i Gjykatës së Apelit për Krimet e Rënda;
84. Vendimi Nr. 56550-00582-00-2009 i Regj. Themeltar, Nr.00-2010-283 i Vendimit (22), datë 20.01.2010 i Kolegjit Penal të Gjykatës së Lartë;
85. Vendimi nr. 41, datë 10.07.2009 i Gjykatës së Apelit për Krimet e Rënda;
86. Vendimi Nr. 56550-00843-00-2009 i Regj. Themeltar, Nr.00-2010-354 i Vendimit (226), datë 10.03.2010 të Kolegjit Penal të Gjykatës së Lartë;
87. Vendimi nr. 66, datë 17.11.2008 i Gjykatës së Apelit për Krimet e Rënda;
88. Vendimi nr. 37, datë 18.04.2016 i Gjykatës së Posaçme të Apelit Kundër Krimit të Organizuar dhe Korrupsionit;
89. Vendimi Nr. 56550-01298-2016 i Regj. Themeltar, Nr. 00-2021-18 i Vendimit, datë 15.01.2021 i Kolegjit Penal të Gjykatës së Lartë;
90. Vendimi nr. 62, datë 23.04.2018 i Gjykatës së Shkallës së Parë për Krimet e Rënda;
91. Vendimi nr. 69, datë 19.09.2018 i Gjykatës së Apelit për Krimet e Rënda;
92. Vendimi nr. 39, datë 18.05.2021 i Gjykatës së Posaçme të Shkallës së Parë Kundër Krimit të Organizuar dhe Korrupsionit;

93. Vendimi nr. 20, datë 25.03.2011 i Gjykatës së Apelit për Krimet e Rënda;

94. Vendimi nr. 45, datë 27.07.2011 i Gjykatës së Shkallës së Parë për Krimet e Rënda;

95. Vendimi nr. 62, datë 07.11.2011 i Gjykatës së Apelit për Krimet e Rënda;

96. Vendimi Nr. 56260-00039-00-2012 i Regj. Themeltar, Nr. 00-2013-1550 i Vendimit (200), datë 12.06.2013 i Kolegjit Penal të Gjykatës së Lartë;

97. Vendimi Nr. 59000-01373-00-2011 i Regj.Themeltar, Nr. 00-2013-1741 i Vendimit (315), datë 22.11.2012 i Kolegjit Penal të Gjykatës së Lartë;

98. Vendimi Nr. 56550-00435-00-2009 i Regj. Themeltar, Nr.00-2010-480 i Vendimit (200), datë 03.03.2010 të Kolegjit Penal të Gjykatës së Lartë;

99. Vendimi nr. 69, datë 23.11.2009 i Gjykatës së Shkallës së Parë për Krimet e Rënda;

100. Vendimi nr. 37, datë 02.10.2010 i Gjykatës së Apelit për Krimet e Rënda;

101. Vendimi Nr. 59000-01401-00-2010 i Regj. Themeltar, Nr. 00-2014-1115 i Vendimit (48), datë 24.02.2014 të Kolegjit Penal të Gjykatës së Lartë;

102. Vendimi Unifikues Penal nr. 3, datë 02.11.2015 i Kolegjeve të Bashkuara të Gjykatës së Lartë;

103. Vendimi nr. 27433/2017 i Seksionit Penal VI të Gjykatës Supreme të Kasacionit të Republikës së Italisë;

104. Vendimi nr. 28252/2017 i Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

105. Vendimi nr. 456, datë 21.09.2012 i Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

106. Vendimi nr. 1147, datë 19.11.2007 i Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

107. Vendimi nr. 41717, datë 06.11.2006 i Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

108. Udhëzimi nr. 1, datë 10.01.1966 i Pleniumit të Gjykatës së Lartë;

109. Vendimi nr. 28252, datë 07.06.2017 të Seksionit Penal IV të Gjykatës së Kasacionit të Republikës së Italisë;

110. Vendimi nr. 36131, datë 25.08.2014 të Seksionit Penal VI të Gjykatës së Kasacionit të Republikës së Italisë;

111. Vendimi datë 22.01.1997 të Seksionit Penal VI i Gjykatës së Kasacionit të Republikës së Italisë;

112. Vendimi nr. 62, datë 23.04.2018 të Gjykatës së Shkallës së Parë për Krimet e Rënda;

113. Vendimi nr. 69, datë 19.09.2018 të Gjykatës së Apelit për Krimet e Rënda;

114. Vendimi nr. 200/2016 i Gjykatës Kushtetuese të Republikës së Italisë;

115. Vendimi nr. 42 datë 05.04.2022 i Mbledhjes së Gjykatës Kushtetuese;

Doktrinë

1. "*Codice Penale Operativo, annotato con dottrina e giurisprudenza*", I Codici Simone OP3, a cura di Luciano Ciafardini, Mario Formisano, Rocco Pezzano, Paolo Scognamiglio, XVII Edizione 2021, Edizioni Giuridiche Simone;

2. "*Il principio del ne bis in idem*", Corte Constituzionale, Servizio studi, Area di diritto comparato, a cura di P. Passaglia, con contributi di C. Guerrero Pico, S. Pasetto, Z. T. Rorig, z. Torrisi;

3. "*E drejta penale*", Pjesa e Përgjithshme, Volumi i Dytë, Luan Hasneziri, Tiranë, 2021, Maluka 2020;

4. "*Diritto penale. Parte Generale.*", Luigi Delpino (magistrate di casazione), Seconda Edizione, Edizioni Giuridiche Simone, Napoli, 2013;

5. "*E drejta penale*", Pjesa e Përgjithshme, Botimi i dytë 2019, Prof. Asoc. Dr. Dorina Hoxha, Prof. Dr. Skënder Kaçupi, Prof. Dr. Maksim Haxhia;

6. "*Commetario breve al Codice di Procedura Penale*", Terza Edizione, G. Cian, A. Trabucchi, Conso Illuminati, Grevi, Giuliani, Wolters Kluwer, Cedam, Breviaria Iuris, Milano, 2020;

Të tjera

https://www.altalex.com/documents/news/2014/07/14/dei-delitti-contro-la-personalita-dello-stato;

https://www.altalex.com/documents/news/2014/04/18/dei-delitti-contro-l-ordine-pubblico;

https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0570;

https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/;

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000024458637/#LEGISCTA000024458641;

https://www.legislationline.org/download/id/6443/file/Spain_CC_am2013_en.pdf;

https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf;

https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx;

https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf;

https://www.crca.al/sites/default/files/publications/Permledhese%20e%20akteve%20nderkombetare%20per%20Drejtesine.pdf;

https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2016&numero=200;

CRIPTOVALUTE E CYBERCRIME. UN CONNUBIO DA NON SOTTOVALUTARE

CRYPTOCURRENCIES AND CYBERCRIME. A COMBINATION NOT TO BE UNDERVALUED

MATTIA ROMANO[1]

Abstract:

La diffusione dello strumento delle criptovalute rappresenta uno dei fenomeni più distintivi dell'era attuale. Esse stanno progressivamente cambiando molti aspetti della vita quotidiana e ad oggi i BitCoin sono accettati come mezzo di pagamento per molti servizi privati e pubblici ed equiparati al denaro in alcuni paesi del mondo. È, dunque, innegabile che le criptovalute rappresentino, grazie all'enorme capitalizzazione di cui godono, una fonte di risparmio molto significativa. Ne consegue la necessità di un elevato grado di attenzione da parte dei legislatori nazionali e sovranazionali al fine di prevenire i reati che possono essere collegati all'uso di queste peculiari valute virtuali. Il presente contributo si prefigge di analizzare le problematiche relative all'accertamento e al perseguimento dei reati connessi all'uso delle valute digitali.

1 *Phd*student in Diritto Penale – Università "*e-Campus"* – corso di dottorato in "Medium e Medialità". Primo segretario della XLII Conferenza dei Giovani Avvocati di Roma. Avvocato del Foro di Roma.

Abstract:

The spread of the cryptocurrency tool represents one of the most distinctive phenomena of the current era. Cryptocurrency has changed every aspect of daily life and to date BitCoins have been accepted as a means of payment for a lot of private and public services and have been equated with money in some countries of the world. Today, therefore, cryptocurrencies represent, thanks to the enormous capitalization they enjoy, a very significant source of savings. It follows the need for a high degree of attention on the part of national and supranational legislators in order to prevent crimes that may be related to the use of these peculiar virtual currencies. The intervention aims to analyze the problematic issues relating to the detection and prosecution of crimes related to the use of digital currencies.

1. Aggiornamento asincrono fra criminalità e Legislatore

Il diritto, com'è noto, ha la funzione di disciplinare e regolare i fenomeni umani e, pertanto, almeno in astratto, dovrebbe evolversi all'unisono con la Società. Tuttavia, molto spesso si rileva un'eccessiva sclerosi del diritto positivo e sovente si ravvisa una manifesta incapacità del Legislatore di novellare le discipline normative in maniera sufficientemente pronta a recepire i mutamenti di quest'epoca.

Chi invece assolve a tale "dovere di aggiornamento" e – per usare una locuzione ben nota agli avvocati – di "formazione continua" è la criminalità che, negli ultimi anni, ha dato prova di aver ben intuito le grandi opportunità di profitto nel settore informatico, prendendo di mira il mercato della rete in costante crescita, trainato dal successo delle criptovalute come il bitcoin, ormai avente un valore estremamente elevato.

Uno dei maggiori rischi correlati all'investimento in dette peculiari valute, oltre a quello – primario – della estrema volatilità del valore di gran parte di esse – è quello correlato al c.d. *phishing* o ad altre condotte illecite poste in essere da criminali 2.0 ai danni degli investitori.

Basti pensare che, secondo una stima di Chainalysis[21], già nell'estate 2016, i danni per gli investitori in criptovalute ammontavano a 225 milioni di dollari: più di 30 mila vittime, con danni ammontanti ad oltre 7.500 dollari ciascuno.

2 Azienda che aiuta le agenzie governative, le aziende di criptovaluta e le istituzioni finanziarie a interagire con sicurezza con la criptovaluta.

In particolare, il tutto avveniva attraverso il ricorso a siti web o social account del tutto simili alle piattaforme di offerta di moneta iniziale, in gergo ICO, mezzo molto utilizzato per raccogliere fondi per nuove criptovalute. In tal modo gli ignari investitori venivano sollecitati ad inviare il danaro che poi veniva illecitamente sottratto dai cyber-criminali.

Recentemente è assurto ai (dis)onori delle cronache un caso che ha avuto una estrema eco mediatica in ragione della rilevantissima entità del danaro sottratto e in ragione della peculiare correlazione della criptovaluta oggetto dell'operazione illecita con la Serie Netflix Squid Game, la serie di successo sudcoreana in cui persone pesantemente indebitate praticano versioni mortali di giochi per bambini allo scopo di vincere denaro.

Nello specifico dal 20 ottobre 2021, in concomitanza con il picco di "viralità" della serie, è stato commercializzato un *token* non ufficiale della prefata serie che ha sin da subito riscosso un estremo successo fra gli investitori con la – erronea – idea che la criptovaluta sarebbe stata un «pay-to-play» per un gioco online, ispirato alla prefata serie di riferimento della valuta.

Il gioco online doveva essere lanciato a novembre e i suoi promotori avevano assicurato che i vincitori sarebbero stati premiati sempre con token Squid.

Tuttavia, dopo essere cresciuto del 310mila% arrivando a valere 2.861 dollari il valore della valuta collassava a 0,003 dollari, con un *market cap* di 2,1 milioni di dollari.

Il tutto solo perché Twitter aveva limitato temporaneamente l'account della criptovaluta per «attività sospette». Di lì a poco diveniva chiaro che l'operazione si era sostanziata in un vero e proprio «rug pull», avendo gli sviluppatori della criptovaluta abbandonato il progetto dopo aver locupletato i danari degli investitori.

Questo solo è uno dei tanti esempi delle nuove modalità operative della criminalità nell'era digitale. Tale esempio dà la misura della estrema e costante necessità per il legislatore di aggiornare la normativa vigente onde contrastare le nuove forme di criminalità.

2. Il doppio volto delle criptovalute.

Gli elevati rischi di commissione di illeciti attraverso lo strumento delle criptovalute sono certamente correlati all'intrinseca opacitàche le

caratterizza.

Basti pensare che le stesse sono, peraltro, sovente utilizzate quale strumento di pagamento nei mercati illegali del *darkweb* e, *ut amplius infra*, per riciclare proventi illeciti.

Appare, dunque, evidente come dette monete virtuali possano essere inquadrate «*nella struttura prismatica del fatto tipizzato*»[3].

Esse possono, dunque costituire tanto oggetto materiale delle condotte di reato, quanto prezzo, prodotto o profittodelle condotte penalmente rilevanti.

Infine, certamente, possono assumere la veste di mera forma di manifestazione onota modale di commissione degli illeciti penali, come nel caso della truffa di cui al paragrafo che precede.

Conseguentemente, è possibile affermarsi che le criptovalute abbiano due distinti livelli di operatività: da un lato possono essere utilizzate quale mezzo alternativo alla moneta tradizionale e, dall'altro, possono costituire il mezzo per la commissione di condotte illecite o il bersaglio delle stesse[4].

In particolare, si è affermato in dottrina come le stesse possano essere qualificate come strumento «a doppio uso»[5]in ragione del fatto che le stessenon di per sé illecite, ma possono essere facilmente utilizzate per scopi illeciti in maniera sistematica ed efficace.

Sicché in questo secondo livello di operatività le criptovalute divengono tratto caratterizzante delle fattispecie criminose.

Tale duplice natura fa sì che non possa in alcun modo ammettersi qualsivoglia automatismoo presunzione di rilevanza penale dell'impiego di criptovalute.

Tuttavia è evidente come l'ordinamento nutra un elevato livello di sospetto verso l'utilizzo di detti strumenti.

In via esemplificativa, il Ministero dell'Economia e delle Finanze ha previsto obblighi di comunicazione di operatività con le criptovalute gravanti sui prestatori di servizi relativi all'utilizzo di valuta virtuale, tanto che si è addivenuti all'istituzione della sezione speciale di cui al comma 8-*bis* dell'art. 17-*bis*, D. Lgs. 141/2010.

---

3 M. Naddeo, *Criptovalute: profili di rilevanza penale*, in *Penale: diritto e procedura*, www.penaledp.it;

4 M. Naddeo, *ibidem.*

5 In tal senso v., L. Picotti, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dr. pen. ec.*, 3-4/2018, p. 605.

Pare, infatti, che il mero utilizzo delle criptovalute possa integrare i "*ragionevoli motivi per sospettare*".

Conseguentemente, laddove in sede di adeguata verifica si riscontri l'utilizzo delle stesse i soggetti obbligati dalla normativa A.M.L. potrebbero essere indotti ad effettuare una S.O.S. onde ridurre i rischi connessi alle eventuali sanzioni correlate alle omesse segnalazioni.

Quanto appena affermato trova riscontro nell'analisi qualitativa delle segnalazioni sintetizzate dal Direttore della UIF all'interno della "*Presentazione del rapporto annuale dell'Unità di Informazione Finanziaria per l'Italia"*[6].

Tale *modus operandi* – laddove foriero di vere e proprie contestazioni penali e non solo di segnalazioni di operazioni sospette – appare, tuttavia, parzialmente confliggente con la natura di *extrema ratio* del diritto penale e con l'argine posto dal principio di offensività che dà la misura oltre la quale non è possibile espandere il diritto penale del rischio[7].

Vanno, infatti, rifuggite tutte le opzioni normative fondate sull'applicazione ipertrofica del principio precauzione.

D'altra parte, una eventuale criminalizzazione preventiva delle mere condotte di utilizzo e scambio delle criptovalute non sarebbe comunque riconducibili alle – purtroppo invalse – tecniche di normazione del pericolo astratto o presunto, in quanto la cui struttura teleologica delle stessefa comunque riferimento a leggi scientifiche o regole di esperienza validate[8].

3. Il rischio di cyberlaundering

Pur essendo stato appena chiarito che sia del tutto erroneo criminalizzare aprioristicamente l'utilizzo delle criptovalute, è, in ogni caso, innegabile che le stesse siano estremamente correlate ad un concreto rischio di commissione di reati di riciclaggio e di fattispecie ad esso affini.

---

6 C.Clemente, *Presentazione del Rapporto Annuale dell'Unità di Informazione Finanziaria per l'Italia (anno 2017)*, in www.uif.it, p. 5. In argomento, E. Messina, *Bitcoin e riciclaggio*, in *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale*, B. Quattrociocchi (*a cura di*), Giappichelli, Torino, 2017, pp. 381 ss.

7 Cfr. M. Naddeo, *op. cit.*che a sua volta richiama C. E. Paliero, *«Minima non curatpraetor». Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Cedam, Padova, 1985, *passim*; C. Sotis, *Il diritto senza codice. Uno studio sul sistema penale europeo vigente*, Giuffrè, Milano, 2007, pp. 207 e ss., nonché pp. 310 ss.

8 D. Castronuovo, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato, «I libri»* di *Archivio penale*, VIII, Roma, 2012, pagg. 40 ss..

Basti pensare che il *report* dell'*Internet Cybercrime Centre* dell'Europol[9]ha evidenziato come vi sia un rapporto diretto tra la capitalizzazione del mercato delle criptovalute e lo sviluppo di fenomeni di riciclaggio digitale o *cyberlaundering.*

Essorappresenta, infatti, la nuova frontiera del riciclaggio e consistenell'utilizzo dei nuovi strumenti tecnologici e telematiciper il riciclaggio dei proventi delittuosi.

Le origini del fenomeno sono strettamente correlate alla progressiva dematerializzazione e informatizzazione dei flussi finanziari che ha fatto sì che vi possano essere scambi di valute senza un previopassaggio per le "canoniche" vie dell'economia tradizionale.

La diffusione e la poliedricità degli utilizzi dei sistemi informatici, basti pensare ai sistemi di*home banking*, ha fatto sì che la rete sia diventato un (non) luogo ideale per il compimento di attività di riciclaggio.

Va, peraltro, evidenziato come si possano riscontrare diverse forme di *cyberlaundering*, quali il riciclaggiodigitale strumentale e il riciclaggio digitale integrale[10].

Il riciclaggio digitale strumentale non è null'altro che un *cyberlaundering*"parziale", in quanto le somme utilizzate per detta operazione riciclatoria non sono *ex ante* dematerializzate.

La c.d. fase di*placement* dei capitali di origine illecita presenta, chiaramente, difficoltà analoghe a quelle sussistenti nelle ordinarie dinamiche del riciclaggio non digitale, essendo necessaria una movimentazione fisica del contante al fine di addivenire alla dematerializzazione dello stesso onde convertirlo in valuta elettronica.

Nel riciclaggio digitale integrale[11], invece, le somme sono già dematerializzate sicché per il riciclaggio delle stesse non si rende necessario un passaggio nella c.d. "realtà materiale".

È chiaro come la ripulitura del denaro *online* sia ben più semplice del riciclaggio nell'economia del mondo materiale, in quanto vi è il vantaggio di poter agire in qualsiasi momento e in pieno anonimato, senza necessità di interfacciarsi *vis a vis* con persone fisiche e con la possibilità di rivolgersi a

9 Il riferimento è all'*Internet Organised Crime ThreatAssessment*(IOCTA) 2017, fruibile sul portale istituzionale al link seguente: *www.europol.europa.eu*.

10 E. Simoncini, Il cyberlaundering: la «nuova frontiera» del riciclaggio, cit., 900.

11 Sul punto si fa rinvio a R. Guttman, *Cybercash: the coming Era of electronic money*, Londra, 2003, 28 ss.; S. Mulinari, *Cyberlaundering*, Milano, 2003, 41.

intermediari sul *web* per il compimento delle operazioni intermedie (*money mules*)[12].

Altro vantaggio del porre in essere le condotte di riciclaggio nel non-luogo del *web* è correlato alla difficoltà nell'individuazione del *locus commissi delicti*e dell'identità dei soggetti coinvolti nelle attività riciclatorie.

Ne consegue che l'utilizzo delle criptovalute permetta una semplificazione di tali attività illecite rendendo assai più semplice la movimentazione delle somme di danaro.

Detto ecosistema digitale e decentralizzato permette, peraltro, di comprimere radicalmente le tempistiche di espletamento delle transazioni, consentendo uno scambio *peer to peer*, senza passare per soggetti terzi gravati dagli obblighi antiriciclaggio[13].

Tutto quanto premesso, occorre porsi un interrogativo di primario rilievo: il *cyberlaundering*è sussumibile nella fattispecie di cui all'art. 648-*bis* c.p. o la contestazione della fattispecie in parola in tali ipotesi non è rispettosa del principio di tassatività?

Le problematiche maggiori attengono in particolar modo alle modalità esecutive della condotta e all'oggetto materiale del reato.

Infatti, se da un lato è vero che la norma incriminatrice del delitto di riciclaggio prevede un reato a forma libera, dall'altro va evidenziato che per l'integrazione della fattispecie in parola vengono valorizzate le modalità della condotta e, in particolare, l'idoneità della stessa a ostacolare l'identificazionedella provenienza illecita del denaro, dei beni o delle altre utilità.

Ne consegue che non residuano dubbi circa la configurabilità del riciclaggio nelle ipotesi di transazioni in valorivirtuali che rendano estremamente difficoltosa la ricostruzione del*digital trial*[14].

Più annosa è, invece, l'individuazione dell'oggetto materialedel riciclaggio delle valute digitali, non essendo ancora stata debitamente individuata in maniera pacifica la natura giuridica da attribuire alle stesse.

Infatti, secondo gran parte della dottrina, allo stato, prevalente, le

12 M. Croce, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *Sistema Penale* n. 4/2021.

13 M. Croce, *Cyberlaundering*, ult. op. cit.

14 L. D'Agostino, Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili diesercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017, cit., 4.

criptovalute non paiono essere assimilabili alle valute*stricto senso* in quanto non aventi corso forzoso né legale[15].

È stato, peraltro, osservato come – ad ulteriore comprova della non assimilabilità di tali valori alla moneta corrente – le*cryptocurrencies*non siano neppure idonee ad assolvere alle funzioni di riserva di valore, unità di conto e mezzo di scambio[16].

Quanto appena affermato porterebbe a ingenerare nell'ermeneuta penalista seri dubbi circa il rispetto del divieto di analogia *inmalampartem*,posto che la tassatività della fattispecie incriminatrice del delitto di riciclaggio parrebbe in tal guisa messa seriamente messa in discussione.

Tuttavia, il pieno rispetto del principio di riserva di legge e dei suoi corollari appena citati, pare ben possibile in ragione della agevole sussunzione delle criptovalute nella categoriaresiduale delle «altre utilità»[17].

In tale nozione possono, infatti, rientrare tutte quelle entità economicamente apprezzabili.

In conclusione, da un lato appare ben possibile ritenere concreto e serio il rischio che le valute virtuali vengano utilizzate per porre in essere condotte riciclatorie e dall'altro appare pacifica la sussumibilità di tali condotte nel paradigma sanzionatorio della fattispecie di cui all'art. 648-*bis* c.p..

Le conclusioni appena condivise evidenziano la necessità di un serio e costante approfondimento del tema da parte dei giuristi accademici e pratici, con conseguente opportunità di una futura integrazione del presente elaborato con ulteriori e ancor più approfondite osservazioni in materia *de qua.*

---

15 Sul punto, cfr. G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,*cit., 417. In tema, G. LEMME – E. S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin,* cit., 24; N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. inf.*, 2015, 1, 450.

16 D. YERMAK, *Is Bitcoin a real currency? An economic appraisal, NBER Working Paper No. 19747,* 2013, 2 ss.

17 S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica,* Milano, 2015, 252; L. STURZO, *Bitcoin e riciclaggio 2.0,* cit., 24.

MBROJTJA JURIDIKO PENALE NDAJ MASHTRIMEVE TË LIDHURA ME KOMPJUTERAT

DR. YLLI PJETËRNIKAJ,
Prosecution Office at First Instance Court of Lezha
Ylli.Pjeternikaj@pp.gov.al

DR. ADNAN XHOLI
Special Prosecution Against Corruption and Organized Crime of Tirana
Adnand.Xholi@spak.al

Abstract

The revolution in information technologies has changed the society fundamentally and will probably continue to do so in the foreseeable future. These developments not only have given rise to unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as ëell as the commission of traditional crimes by means of new technologies.

The new technologies challenge the existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory.

The efficiency in the fight against cybercrime requires diffferent states to have a common unified material and procedureal approach. This was the Council of Europe's aim in undertaking a legislative initiative, which

concluded with the adoption of the Convention "On Cyber Crime", in order to achieve the widest possible unity among its members, as ëell as the most extensiveinternational co-operation in criminal matters, rapid and effective.

The Council of Europe adopted the Convention "On Cyber Crime" in Budapest, on 23.11.2001. A total of 58 countries have signed the Convention, 28 countries have ratified it. The Convention was ratified by Albania by law no. 8888, dated 25.04.2002 "On the Ratification of the Convention on Cyber Crime".

With the ratification of the Budapest Convention, Albania undertook the responsibility and obligation to criminalize the acts of computer-related fraud. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property. In this work we will analyze the techniques of the criminalization of the penal act of computer fraud, as ëell as the harmonisation with the approach required by international instruments. We will also analyze the problems encountered in jurisprudence regarding legal qualifications, as well as fundamental differences through this criminal activity and those similar to it.

Keywords: fraud, computer, cybercrime, convention, criminalization.

Hyrje

Zhvillimet e fundit të teknologjisë së informacionit[1], të kombinuar me zgjerimin e shpejtë të përdorimit të sistemeve të kompjuterike dhe telematike, ka bërë që ligjvënësi, në nivel global, të përballet me problemin që lind nga nevoja për të disiplinuar ngjarje (kibernitike) "të panjohura" më parë.[2] Pasojat ekonomike të shkaktuara nga kryerja e krimeve teknologjike dhe informacionit kërkojnë ndërhyrje të menjëhershme nga autoritetet shtetërore dhe komunitare për të rregulluar një fushë në zgjerim progresiv.[3]

Përhapja e përdorimit të internetit, "rrjeteve sociale", kërkon reagime të

1 Shih Corrias L., "Informatica e Diritto Penale: elementi per una comparazione con il diritto statunitense", 1987.

2 Shih Giovanni Modesti, "Il reato di frode informatica" Una rilettura alla luce delle recenti pronunce giurisprudenziali, aksesuar me datë 09.06.2022 në adresën: http://www.apihm.it/pdf/IlReatoDiFrodeInformatica.pdf

3 Shih Vaccaio D., L'evoluzione del concetto di misura di sicurezza a protezione del sistema informatico alla luce dell'art. 615-ter e del Disciplinare Tecnico; in www.computerlaw.it,; 2022;

caktuara dhe sistematike, mbi të gjitha, për sa i përket legjislacionit penal, reagime të tilla duhet të koordinohen në nivel të komunitetit mbishtetëror, duke qenë se ky është një fenomen që nuk mund të kufizohet, pikërisht për shkak të veçorive që ka, në një gjendje të vetme.[4]

Në vitet '80 dhe '90 të shekullit të kaluar, zonat makro që filluan të trajtojnë fenomenin në terma sistematikë ishin Amerika e Veriut dhe Evropa.[5] Qasja e SHBA-ve[6] ishte të fillohej nga përcaktimi i definicioneve për termat e përdorur për të përshkruar këto raste (kompjuter, pajisje elektronike[7], sistemi kompjuterik[8], sistemi telematik[9], malware[10], etj.) dhe më pas të identifikonte se në cilat fusha është e nevojshme marrja e masave, duke u bërë një dallim i qartë midis legjislacionit federal dhe atij të miratuar nga shtete individuale.

Në Evropë, përveç Britanisë së Madhe, e cila nisi rrugën e saj në vitet

---

4 Shih Pomante G., Frode informatica, la soluzione arriva dall'art. 640 ter, su www.pomante.com,

5 Shih Logroscino S. Analisi e considerazioni sul delitto di Frode informatica quale autonoma figura di reato rispetto al delitto di Truffa , www.diritto.it (2011);

6 Shih Romani M. e D. Liokopoulos, La globalizzazione telematica. Regolamentazione e normativa nel diritto internazionale e comunitario, ed. Giuffrè, (2009)

7 Shih Salvatori I., L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cooking, in Rivista Italiana di Diritto e Procedura Penale, (2008)

8 Karakterizohet nga lejimi i përpunimit dhe organizimit të të dhënave, të cilat mund të përdoren për qëllime të ndryshme. Ky term përfshin softuerin bazë (që lejon kompjuterin të funksionojë), softuerin aplikativ (që i mundëson përdoruesit të shkruajë tekste, të vizatojë grafika etj.). Cass. Seksioni VI, 4 tetor 1999 dha përkufizimin e mëposhtëm: "*një sistem kompjuterik ose telematik, që do të thotë, nga ky i fundit ... një grup pajisjesh të destinuara për të kryer çdo funksion të dobishëm për njeriun, nëpërmjet përdorimit, qoftë edhe të pjesshëm, të teknologjive të teknologjisë së informacionit, të cilat karakterizohen - me anë të një veprimtarie "koduese" dhe "dekoduese" - nga "regjistrimi" ose "ruajtja", me anë të impulseve elektronike, në mbështetje adekuate të "të dhënave", pra paraqitje elementare të një fakti, të kryera nëpërmjet simbolet (bitet), në kombinime të ndryshme, dhe përpunimi automatik i të dhënave të tilla, për të gjeneruar "informacion", të përbërë nga një grup pak a shumë i madh të dhënash të organizuara sipas një logjike që u lejon atyre të shprehin një kuptim të veçantë për përdorues*".

9 Ai përbëhet nga një mori sistemesh kompjuterike të lidhura me njëri-tjetrin për të lejuar transmetimin dhe komunikimin në distancë të informacionit.

10 Në sigurinë kompjuterike, termi malware përgjithësisht tregon çdo softuer të krijuar me qëllimin e vetëm për të shkaktuar dëme pak a shumë serioze në një kompjuter ose sistem kompjuterik në të cilin ai funksionon. (marrë nga: WIKIPEDIA) Viruset dhe krimbat janë pjesë e këtij lloji sulmi me ndryshimin e mëposhtëm: ndërsa viruset kërkojnë disa veprime nga ana e përdoruesit për t'u përhapur, krimbat janë programe vetë-përsëritëse që, pasi ekzekutohen, përhapen pa ndërhyrje. të atyre që i krijuan.

1990, duke identifikuar një sërë hipotezash të sjelljes kriminale, imputi erdhi nga legjislacioni i BE-së, i cili veproi si një udhëzues ndaj Shteteve Anëtare. Në Itali me ligjin nr. 547, datë 23.12.1993, u miratua reforma kibernitike, e bazuar në Rekomandimin e Këshillit të Evropës të vitit 1989.[11]

Ndërsa në Shqipëri reforma penale lidhur me krimin kibernitik është realizuar në vitet 2008, disa vite pas ratifikimit të konventës së Budapestit. Në kuadër të kësaj reforme, ndërsa masat penale kriminalizuese ishte parashikimi i figurës së vepres penale të "Mashtrimi kompjuterik" në seksionin e II të titulluar "Mashtrimet", në Kreun III titulluar "Vepra penale kundër pasurisë dhe në sferën ekonomike".[12] Ligjvënësi ynë ka mbajtur në konsideratë orientimet e dhëna nga konventa e Budapestit lidhur me hipotezën e normës juridike që duhet të kishte kriminalizimi i figurës së vepres penale të "Mashtrimet e lidhura me kompjuterat".[13]

Ndërmarrja e një masë të tillë penale materiale, ka rëndësi të madhe praktike, sepse mashtrimi kompjuterik në realitetin shqiptar ka pësuar një rritje të ndjeshme, duke shfaqur në pjesën dërrmuese të tij edhe karakter transnacional, dhe sjellë pasoja tepër të rënda për individetet dhe qarkullimin civil.[14] Në mungesë të nismës ligjore, sjellje të tilla, shoqërisht të rrezikshme, krijonin veshtirësi gjatë operacionit intelektual të kualifikimit ligjor sipas

---

11 Rekomandimi nr. R 899 i Komitetit të Ministrave për shtetet anëtare për kriminalitetin kompjuterik, miratuar për Komitetin e Ministrave më 13 shtator 1989, në mbledhjen e 428-të të Zëvendës Ministrave.

12 Shtuar me ligjin nr. 10 023, datë 27.11.2008. Në nenin 143/b të K.Penal, në seksionin që trajton veprat kundër pasurisë dhe në sferën ekonomike, me përmbajtjen si më poshtë:"*Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet. Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.*"

13 Në nenin 8 të Konventës "Për krimin në fushën e kibërnitikës", titulluar "Mashtrimet e lidhura me kompjuterat", është parashikuar se: *Çdo Palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, shkaktimin e humbjes së pasurisë të një tjetri nëpërmjet:*
a) futjes së ndonjë të dhëne, ndryshimin, fshirjen apo heqjen e të dhënave kompjuterike;
b) ndonjë interferencë me funksionimin e një sistemi kompjuterik, me synimin e pandershëm e mashtrues për prokurimin pa të drejtë të një përfitimi ekonomik për veten apo për një tjetër."

14 Shih Ismet Elezi, "E drejta penale e Republikës së Shqipërisë (Pjesa e posaçme)", fq. 245.

linjave tradicionale kriminalizuese.

Mashtrimi kompjuterik kriminalizon sjelljet e kryera, të pakundërdrejtuara një personi, por, nëpërmjet manipulimit të një sistemi kompjuterik (duke ndryshuar ose ndërhyrë në një sistem kompjuterik ose telematik, apo në të dhëna, informacione apo programe të përdorura prej tyre), cenon të drejtat pasurore, duke përfshirë të gjitha mjetet dhe instrumentet financiare që mund të menaxhohen edhe nëpërmjet kompjuterit, ose internetit,[15] dhe sjell përfitim të një fitimi të padrejtë, duke dëmtuar të tjerët.

1. Interesat juridike të mbrojtura, karakteri multiofensiv dhe natyra e vepres penale

Duke marrë në konsideratë seksionin, i cili përcakton objektin grupor, apo pozicionin e dispozitës ndërmjet të tjerave, duke ndikuar edhe në karakterizimet e objektit të drejtëpërdrejtë, deduktohet se objekti juridik i mbrojtjes së figurës së mashtrimit kompjuterik përfshin mbrojtjen e aktiveve/mirave, të kuptuara si grupi i të gjitha atyre burimeve financiare "të paprekshme", (psh, paratë dhe letrat me vlerë të depozituara në një llogari rrjedhëse të një banke, e cila i menaxhon ato nëpërmjet një sistem kompjuterik), që mund të aksesohen edhe nëpërmjet një sistemi kompjuterik.[16]

Në këtë përcaktim marrin rëndësi, *së pari*, ekzistenca e të dhënave kompjuterike dhe së *dyti,* konstatimi tregues i natyrës strukturore, e "klonuar" mbi atë të figurës së mashtrimit klasik[17] sipas nenit 143 të Kodit Penal, dhe së *treti*, *prejardhja* e tij , duke pasur parasysh se në vitin 2008, ligjvënësi vendosi ta prezantojë atë, sepse konstatoi se mashtrimi, i ndërtuar mbi gënjeshtren, apo shpërdorimin e besimit të një personi, ishte i papërshtatshëm për kriminalizimin e mashtrimit të kryer nëpërmjet manipulimit të sistemeve kompjuterike ose të të dhënave[18], e kërkuar edhe nga Bashkimi Evropian, i cili e konsideroi të nevojshme vënien përballë mashtrimit tradicional (neni 143 të Kp) të një normë e re që ishte në gjendje të plotësonte atë që dukej si një boshllëk serioz në sistemin penal, i paaftë për të kundërshtuar në mënyrë

15 Shih Di Stefano Logroscino La frode informatica quale autonoma figura di reato rispetto al delitto di truffa", Pubblicato il 05/01/2012

16 Shih Mantovani, F., Diritto penale, pt. spec., II, Delitti contro il patrimonio, III ed., Padova, 2009, fq 210.

17 Shih Pecorella, C., Il diritto penale dell'informatica, rist. con aggiornamento, Padova, 2006, fq 63

18 Shih Cass. pen., sez. II, 24.2.2011, n. 9891, in DeJure

adekuate fenomenin e përhapur të të ashtuquajturit mashtrim kompjuterik[19]

Nga ana tjetër, megjithatë, duke pasur parasysh se krimi i referuar në nenin 143/b , është një krim tipik kompjuterik, nëse i kushtohet vëmendje sjelljes së inkriminuar nga kjo nuk mund të anashkalohet se e njëjta dispozitë mund të konsiderohet gjithashtu se synon mbrojtjen, qoftë edhe vetëm në mënyrë indirekte, të "funksionimi i rregullt i sistemeve kompjuterike dhe telematike"[20], si dhe "konfidencialiteti që duhet të shoqërojë përdorimin e tyre"[21], të cilat janë aktive të mbrojtura drejtpërdrejt nga rregullat që ndëshkojnë dëmtimin e sistemeve kompjuterike (nenet 293/b e vijues të KP), hyrja e paautorizuar kompjuterike (neni 192/b), falsifikimi kompjuterik (neni 186/a) dhe përgjimi i paligjshëm i të dhënave kompjuterike.[22]

Megjithatë, duke qenë se rastet inkriminuese të krimeve kompjuterike kanë të gjitha një element të përbashkët që është "qasja" e të bërit të dallimit ndërmjet "krimeve të aksesit", në të cilat paligjshmëria përfundon në të, dhe "krimet e kryera përmes aksesit", në të cilat aksesi, qoftë i ligjshëm apo abuzive, nuk është i rëndësishëm në vetvete, por është instrumental për qëllime të tjera të mëtejshme ose veprime të paligjshme të tjera". Mashtrimi kompjuterik duhet të vendoset në kategorinë e dytë të krimeve kompjuterike, nga deduktohet se objekti parësor i mbrojtjes është ndëshkimi i "sjelljeve kompjuterike" që shkaktojnë dëme financiare dhe ekonomike, qoftë edhe nëpërmjet vetëm lëvizjes të informacionit ose të dhënave.[23]

Është e nevojshme të kuptohet se krimet kompjuterike mbrojnë një aset ligjor unitar, të kuptuar si " *paprekshmëri kompjuterike* ", e përcaktuar si " *nevoja për të mos ndryshuar marrëdhënien triadike midis të dhënave të realitetit, informacionit përkatës dhe subjekteve që kanë të drejtë të përpunohen. kjo e fundit në fazat e ndryshme të saj (krijim, transferim, marrje)" [24] ,* ose edhe si *"aktiv jo-material me karakter të drejtë reale, pra e drejtë e qenësishme ndaj aktivit që përfaqëson objektin e tij* ".[25] Mund të argumentohet se e mira juridike unitare e *krimeve kompjuterike* është

19 Shih Mucciarelli, F., Commento all'art. 10 della l. n. 547 del 1993, in Legisl. pen.,1996, fq 136

20 Shih Cass.pen sez. V n. 1727 datë 30.09.2008 , R.U. (rv. 242938)

21 Shih Antolisei, F., Manuale di diritto penale, pt. spec., I, XV ed., Milano, 2008, fq 386.

22 Shih nenin 293/a të Kodit Penal.

23 Shih Pica, G., Internet, in Dig. pen., Aggiornamento, I, Torino, 2007, fq 433.

24 Shih Militello, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in *Rivista trimestrale di diritto penale dell'economia,* 1992

25 Shih Frosini, V., *Il Disegno di legge sulla repressione dei reati informatici*, in *Informatica e documentazione*, 1993, 1 e 2

prirja për të mbrojtur të drejtën e konfidencialitetit, megjithëse nga koha e hyrjes në fuqi të normës, do të dukej ende herët për të pohuar se përdorimi i teknologjive të informacionit, i lirë nga çdo manipulim, mund të cilësohet ligjërisht si e drejtë e "personalitetit" në lidhje me lirinë e kompjuterit, dhe, për rrjedhojë, si një e drejtë me vlerë për mbrojtje juridike penale.[26] Prandaj disa autorë argumentojnë se interneti "*shënon lindjen e një situate të re subjektive juridike ose, më saktë, të aspektit aktiv të saj: 'të drejtën aktive të lirisë së kompjuterit', domethënë ndërveprimin njeri-makinë që lejon dërgimin dhe marrjen e informacionit, i cili shtohet, plotësohet, për të drejtën pasive të lirisë së kompjuterit, e cila përkon me mbrojtjen e konfidencialitetit të të dhënave personale, të cilat mund të dëmtohen nga potenciali i përhapjes së internetit* " [27] .

Mashtrimi kompjuterik është parashikuar për të mbrojtur asetet ligjore të ndryshme nga asetet, të tilla si, në veçanti, interesi për konfidencialitetin në përdorimin legjitim të sistemeve IT dhe telematike, si dhe interesi për funksionimin e rregullt të sistemit, (IT ose telematike), të cilat gjtihashtu përbejnë një fokus dytësor, apo tretësor të tij.

2. Teknika e inkriminimit alternativ. Nocione dhe veçori të faktit tipik penal.

Nga këndveshtrimi i elementëve të anës objektive figura e veprës penale të mashtrimit kompjuterik ka një strukturë të dyfishtë pasi mund të konsumohet në mënyrë alternative me anë të ndërhyrjes në funksionimin e një sistemi kompjuterik ose me anë të futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike.[28]

Sjellja tipike përbëhet nga: *a*) ndryshimi "në çfarëdo mënyre i funksionimit të një sistemi IT dhe telematik"; dhe *b*) ndërhyrja "pa të drejtë në çdo mënyrë mbi të dhënat, informacionin ose programet e përfshira në një sistem kompjuterik ose telekomunikacioni ose në lidhje me të".[29] Megjithatë, të dy

---

26 Shih V. Rombo, *Crimini informatici alla luce dei nuovi approdi legislativi*, on-line su www.ceasonline.com/it/.

27 Shih Fiandaca-Musco, *Dir. Pen. P. s.*, *I delitti contro il patrimonio*, Bologna, 2002; PAGLIARO, *Principi di diritto penale*, *P. s.*, *Delitti contro il patrimonio*, Milano, 2003; Antolisei, *Manuale di diritto penale, P.s.*, I, Milano, 2002. Si veda anche MASI, *Frodi informatiche e attività bancaria, in Rivista penale dell'economia,* 1995*,* il quale sostiene che l'oggetto della tutela nel delitto ex art. 640 ter c.p. sia la libertà negoziale.

28 Shih Vendim nr. 995, datë 23.04.2014 i Gjykatës së Shkallës së Parë Tiranë.

29 Shih Pecorella, C., Commento Art. 640 ter c.p., in Codice penale commentato, Artt.

sjelljet tipike marrin rëndësi penale vetëm nëse lejojnë që të arrihet një fitim i padrejtë me dëmtimin e të tjerëve, e derterminuar nga natyra materiale e kësaj vepre penale, e theksuar në termat: "kushdo që, duke ndryshuar ... ose duke ndërhyrë ... prokuron për vete ose të tjerët një fitim të padrejtë me dëm të të tjerëve".[30]

Veprimi i "ndryshimit" ndikon në funksionimin e kompjuterit ose të sistemit telematik (psh ndryshimi i mënyrës së hyrjes dhe daljes nga sistemi i një website i caktuar, i tillë që, nëse kompjuteri do të mbetej i lidhur me rrjetin dhe faqen, pavarësisht nga mendimi i përdoruesit se ka dalë nga llogaria, kjo do të sillte një përfitim të padrejtë për administruesin e faqes dhe, në mënyrë spekulative, dëm ekonomik për përdoruesin). Në këtë aspekt duhet të theksohet se "*ndërhyrja manipuluese duhet të jetë e tillë që të modifikojë qëllimet, për të cilat synohet sistemi kompjuterik, por krimi ndodh edhe kur duke respektuar qëllimin e synuar të sistemit, përmbajtja e tij është e manipuluar (omissis) "*.[31]

Ndryshimi i një sistemi kompjuterik ose telematik, i cili mund të kryhet "në çfarëdo mënyre", do të ndodhë sa herë që ka pasur një manipulim, i cili ka modifikuar me mashtrim mënyrën e rregullt të funksionimit të sistemit.[32] Ndryshimet në sistemet kompjuterike ose telematike kryesisht përbëhen nga manipulime të programeve, d.m.th. softuerit, që kompjuterët përdorin për të përpunuar të dhënat dhe informacionin dhe mund të kryhen ose nëpërmjet modifikimit të pjesshëm ose të plotë të programit, zakonisht, i përdorur, si nëpërmjet ballafaqimit, mbivendosjes ose në kundërshtim me këtë të fundit të programeve të tjera.[33]

Sjellja alternative e 'ndërhyrjes pa të drejtë' synon të dhëna, informacion (dmth. për të thjeshtuar, një grup të dhënash) ose programe (*softuer*) të instaluara në *harduer*. Në veçanti, duhet theksuar se ndërhyrja, për t'u harmonizuar me sjelljen e përshkruar nga hipoteza e nenit 143/b i Kodit Penal, duhet të bëhet " *pa të drejtë"* dhe, për rrjedhojë, jo vetëm në mungesë të pëlqimit të nevojshëm të pronarit të të dhënave, informacionit dhe programeve të përfshira në sistemin kompjuterik, por edhe në një mënyrë

575-734 bis, a cura di E. Dolcini e G. Marinucci, III ed., Milano, 2011, 6417

30 Shih nenin 143/b të Kodit Penal

31 Shih S. Deśtito, G. Dezzani, C. Santoriello, *Il diritto penale delle nuove tecnologie*, Padova, 2007

32 Shih Pecorella, C., Commento Art. 640 ter c.p., cit., 6417

33 Shih Cass. pen., sez. V, 19.3.2010, n. 27135, in DeJure,

" *që nuk lejohet nga rregulloret ligjore ose burime të tjera, (omissis))"* [34].

Sjelljet "ndërhyrje" në të dhëna, informacione dhe programe, dmth modifikimi i përmbajtjes, apo edhe i funksionit të këtyre komponentëve të ndryshëm të një kompjuteri, ose sistemi telematik, janë të rëndësishme, siç u përmend tashmë, vetëm nëse personi që ndërhyn e bën këtë "pa të drejtë". Ndërhyrje "pa të drejtë", nuk është vetëm ajo e atij që ndërhyn në mënyrë të paligjshme, pa asnjë të drejtë, por edhe e atij që vepron duke përdorur "keq", apo edhe duke abuzuar me një të drejtë që realisht e zotëron. Nisur nga këto premisa, është e qartë se paligjshmëria e ndërhyrjes përfaqëson një element tipik të faktit, në mungesë të të cilit fakti nuk mund të mos konsiderohet atipik.

Pavarësisht sjelljes alternative inkriminuese ligjvënësi nuk është kujdesur që të dyja të përfshijnë nocionin e lirë të sjelljes tipike, për të qënë gjithëpërfshirës. Kjo deduktohet nga mungesa e termit "në çfarëdo mënyre " , kjo do t'i jepte kësaj hipotezë, mos kërkimin e ndonjë sjellje specifike.[35]

Në mashtrimin kompjuterik, të vepruarit "pa të drejtë" është një element i faktit tipik, për këtë arsye personi që vepron në ushtrimin e një të drejte, të ushtruar drejt, sjell në jetë një fakt të ndryshëm nga ai i përshkruar nga rast abstrakt. Veprimi në ushtrimin e një të drejte, pra, të ushtruar drejt, nuk përjashton, sepse eliminon, në rrjedhën e sipërme, tipikitetin.[36]

Manipulimet e të dhënave nga ana e *jashtme* zbulojnë, nëse ato kanë të bëjnë me të dhënat, informacionin dhe programet e përfshira në një sistem kompjuterik ose telematik, ose nëse kanë të bëjnë me të dhënat, informacionin dhe programet "përkatëse" për një sistem të tillë: dhe, duhet të të konsiderohen të gjitha ato të dhëna të cilat, pavarësisht se janë të përfshira në mbështetje materiale "të jashtme" (të tilla si, për shembull, *CD* , apo edhe *floppie*) janë ose *hyrje* , domethënë të dhëna dhe informacione që duhet të futen në sistem në mënyrë që ai të mund të procesi, ose *prodhimi* , të cilat janë të dhënat që kompjuteri ka përpunuar tashmë dhe, për rrjedhojë, rezultatet e përpunimit.[37]

---

34 Shih Di Stefano Logroscino **"**La frode informatica quale autonoma figura di reato rispetto al delitto di truffa", Pubblicato il 05/01/2012

35 Shih Dello Iacono, *Articolo 640 ter: truffa o furto? La Frode informatica e il «modello 640»*, in *Temi Romana*, 1996. Di orientamento opposto C. PECORELLA, *Diritto penale dell'Informatica,* Padova, 2006

36 Shih Mantovani, F., op. cit., 201; nonché Pica, op. ult. cit., 146; cfr., sul consenso dell'avente diritto nella violazione di domicilio, Cadoppi, A.-Veneziani, P., Elementi di diritto penale, II ed., Padova, 2004, fq 239

37 Shih Pecorella, C., Commento Art. 640 ter c.p., cit., 6418

Nën konceptin e ndërhyrjes në funksionimin e programit apo sistemit përfshihen akte të tilla si manipulimi i pajisjeve, heqja e printimeve apo akte që ndikojnë në regjistrimin ose rrjedhjen e të dhënave, ose sekuencën në të cilën veprojnë programet.[38] Ndërhyrja mund të bëhet me ndërhyrje fizike apo logjike që çojnë sistemin në gabim. Pra, për shkak të ndërhyrjes sistemi nuk kryen në rregull apo sipas udhëzimeve veprimet për të cilat është destinuar.

Futja e të dhënave kompjuterike duhet kuptuar si futje e të dhënave kompjuterike, të sakta ose jo, në mënyrë që ato të ndikojnë në sistem dhe të sjellin një përfitim për autorin dhe rrjedhimisht pakësim në pasurinë e të dëmtuarit. Ndërsa ndryshimi i referohet modifikimeve apo ndryshimeve të pjesshme të të dhënave. Fshirja dhe heqja e të dhënave megjithëse duken si sinonime të njëra tjetrës, dallojnë në faktin se fshirja konsiston në "largimin" e të dhënave nga një medium kurse heqja konsiston në fshirjen e tyre.

Duke qenë se sistemit kompjuterik i mungon aspekti psikologjik, që shoqëron individin inkriminohen ndërhyrjet në funksionim dhe futjet pa të drejtë në përmbajtje, përmes të cilave arrihet të sigurohet një përfitim. Pavarësisht dallimeve, sjellja e dënueshme në të dyja format e shfaqjes së mashtrimit mbetet ajo e nxjerrjes së një përfitimi në dëm të të tjerëve.[39]

Vepra konsiderohet e konsumuar edhe kur destinimi i sistemit nuk ndryshohet, por ndërhyhet në përmbajtje, duke prekur gjithsesi funksionimin. Në rastin e mashtrimit kompjuterik nuk është e nevojshme që sistemi të jetë i mbrojtur nga masa sigurie që vepra të konsiderohet e kryer.[40] Elementi kryesor i veprës është pasoja-përfitimi. Në raportin shpjegues të Konventës së Budapestit, është sqaruar se mashtrimet kompjuterike konsiderohen të konsumuara nëse prodhojnë një humbje të drejtpërdrejtë ekonomike në pasurinë e një personi, dhe autori ka vepruar me qëllimin për t'i siguruar vetes një përfitim të paligjshëm pasuror për vete ose për një person tjetër. Termi humbje apo pakësim i pasurisë, është një nocion i gjerë, i cili përfshin humbjen e parave, të pasurive të luajtshme apo të paluajtshme ekonomikisht të vlerësueshme.[41]

---

38 Council of Europe, European Treaty Series - No. 185, Explanatory Report to the Convention on Cybercrime, fq. 15.

39 Shih Erida Visoçi "Analizë juridiko penale materiale e krimit kompjuterik në këndvështrim teorik, praktik e krahasimor", Shkolla e Magjistrtures, Tirane 2017, fq 43

40 Shih Cass.pen.sez n. 6958 e 25-01-2011 (seanca e 25-01-2011), (rv. 249660)

41 Council of Europe, European Treaty Series - No. 185, Explanatory Report to the Convention on Cybercrime, fq. 15

Mashtrimi kompjuterik është një krim tipik i ngjarjes, sepse "ndryshimi" i sistemit dhe "ndërhyrja" në të dhëna (të cilit neni 143/b i referohet duke përdorur shprehjen "ndryshim ... ose ndërhyrë ... prokurë") mund të konsiderohen tipike vetëm kur janë të lidhura etiologjikisht, në një marrëdhënie shkak-pasojë, me ngjarjen, të cilën ligji e identifikon shprehimisht në arritjen e një fitimi të padrejtë për veten ose për të tjerët, por që duhet të ndahet në dy ngjarje të dallueshme, sepse fitimi i padrejtë duhet të jetë shkaktuar nga ana e tij nga "rezultati i parregullt i procesit të përpunimit".[42]

Lidhur me padrejtësinë e fitimit, gjithçka ka lidhje me llojin e mashtrimit, duke marrë rëndësi, në profil i dyfishtë, sepe sjellja mund të konsiderohet tipike vetëm kur lejon arritjen e një fitimi të padrejtë, i cili nga ana e tij i shkakton dëm financiar të dëmtuarit. Në mashtrimin kompjuterik dëmi merr tiparet e një ngjarjeje të dytë reale, e cila nuk është e njëjtë me fitimin, me të cilin duhet të vendoset në një marrëdhënie shkak-pasojë.

3. Problematikat e shfaqura në praktikë lidhur me kualifikimin juridik të këtij fakti tipik.

Në doktrinën juridike dhe në juriprudencën e vendit tonë nuk ka qënë e lehtë për të identifikuar, në kuadër të kualifikimit ligjor, rastet e mashtrimit kompjuterik nga ato të konsumimit vetëm të mashtrimit në kuptimin klasik të tij, apo si dhe rastet e konkurimit të kësaj figure të vepres penale, me ato të cilat e shoqërojnë ose pasojnë atë, ose me të cilat është e ngjashme.

Kështu veshtirësitë qëndrojnë në përcaktimin e figurës së vepres penale të konsumuar, ndërmjet mashtrimit kompjuterik dhe figurave të tjera, tek të cilat ana objektive e tyre është e ngjashme me anën objektive të tij, si dhe përcaktimin të momentit, nga i cili vepra penale konsiderohet e konsumuar. I tillë është rasti i pronarit të një *arcade game*, i cili zëvendëson kartën e videolojës e krijuar për të fituar një përqindje prej 25%, me një tjetër që lejon fitime jo më shumë se 5%. Dilema e kualifikimit ligjor ka krijuar diskutime teorike dhe praktike. Duke u nisur nga ana objektive që një veprim i tillë e bën klientin, i cili nuk ka dijeni për një truk të tillë, të luante dhe të humbiste më shumë sesa do të donte, ose më mirë do të duhej të kishte, duke u kundërdrejtuar direkt vullnetit të individit, kondicionon kualifikimin ligjor sipas figurës së vepres penale të mashtrimit në kuptimin tradicional.[43] Nëse

42 Shih Picotti, L., Reati informatici, in Enc. Giur. Treccani, Torino, 1991, fq. 27

43 Shih Vendimin e Gjykatës së Kasacionit të Italisë, sez. I, 24.2.2012, n. 11473, in DeJure

sistemi kompjuterik i falsifikuar përmban, gjithashtu, një modifikim të aftë për të dërguar të dhëna të pavërteta mbi vëllimin e lojës në zyrën e taksave, atëherë do të kemi konkurim ndërmjet mashtrimit në dëm të lojtarit dhe mashtrimit kompjuterik në dëm të shtetit.[44]

Në këtë aspekt rëndësi të veçntë merr analiza krahasuese e këtyre dy figurave të veprave penale, që synon të evidentojë elementet diferencues, si dhe ato të përbashkëta ndërmjet rasteve të përshkruara përkatësisht nga nenet 143 dhe 143/b të Kodit Penal. Duhet theksuar se krimi i mashtrimit kompjuterik përbën një rast të veçantë, figurë specifike në lidhje me mashtrimin, i cili është figurë e përgjithshme, duke u konsideruar si një hipotezë autonome e krimit.

Lidhur me relacionin ndërmjet këtyre dy figurave të vepres penale, për ekzistencën e një marrëdhënieje *specifike/ të përgjithshme* doktrina e së drejtës penale ka patur qëndrime të ndryshme. Disa autore argumentojnë se mashtrimi kompjuterike, do të përbënte një hipotezë të një krimi të veçantë në lidhje me atë të përgjithshëm të mashtrimit.[45] Megjithatë, ky supozim nuk mund të pranohet, sepse mashtrimi kompjuterik, në lidhje me krimin e mashtrimit, paraqet elemente autonomie të tilla që e bëjnë të pamundur strukturialisht ekzistencën e një marrëdhënie specialiteti midis dy veprave penale.[46]

Në veçanti, në lidhje me mashtrimin kompjuterik nuk ka asnjë referencë për një sjellje që është e lidhur, me anë të artifikimeve ose mashtrimeve që synojnë të mashtrojnë personin e dëmtuar (ose palën e tretë) dhe ta bëjnë atë të kryejë një akt tjetërsimi të aseteve që përndryshe nuk do të realizohej. Mashtrimi kompjuterik përfshin një sjellje të ndryshimit të funksionimit të kompjuterit ose sistemit telematik, apo të ndërhyrjes abuzive në të dhëna, informacion ose programet që përmban, duke drejtuar sjelljen e tij mashtruese drejtpërdrejt në kompjuter ose në sistemin telematik. Për rrjedhojë ngjarjet e përfitimit të padrejtë dhe dëmtimi i të tjerëve rrjedhin drejtpërdrejt nga ky veprim. Megjithatë, pavarësisht autonomisë së këtyre figurave të vepres penale, ato kanë elementë të përbashkët, në veçanti nëse i referohemi përfitimit të padrejtë dhe dëmtimit të të tjerëve.

Këto dallime dhe të përbashkëta ndërmjet tyre janë evidentuar edhe nga praktika e gjyqësore. Gjykata e Kasacionit të Italisë, lidhur me strukturën

44 Shih Vendimin e Gjykatës së Kasacionit të Italisë, sez. V, 19.3.2010, n. 27135, in DeJure

45 Shih G. Pica , *Diritto penale delle tecnologie informatiche*, *op. cit*

46 Shih G. Fiandaca, E. Musco, *Diritto penale, parte generale, op. cit*

e krimit të mashtrimit kompjuterik, ka arsyetuar se: *".....krimi i mashtrimit kompjuterik, i cili postulon domosdoshmërisht manipulimin e sistemit, ka të njëjtën strukturë dhe të njëjtët elementë përbërës të mashtrimit, me të vetmin ndryshim se nuk mashtrohet personi i dëmtuar, por veprimtaria mashtruese e subjektit aktiv manipulon sistemin e IT-së...."*.[47]

Lidhur me autonominë vepres penale të mashtrimit kompjuterik, Gjykata e Kasacionit së Italisë argumenton se: "....*Është i padyshimtë (omissis) që mashtrimi kompjuterik integron një figurë autonome të krimit, ndryshe nga sa është konsideruar në jurisprudencë në lidhje me hipotezën e mashtrimit....."* .[48]

Nga ana tjetër, mashtrimi kompjuterik duhet të përjashtohet në rastin kur subjekti aktiv për të hyrë në një apartament për të vjedhur, hap një bravë elektronike, duke futur një kod të rremë ose një kartë të falsifikuar.[49] Është i qartë kualifikimi sipas vepres penale të vjedhjes.[50] Doktrina e së të drejtës penale dhe jurisprudenca i ka trajtuar në të njëjtin linjë arsyetuese edhe rastet e sjelljes, për shkak të "llojit kriminal"[51]rastet e vjedhjes së një paketë cigaresh ose një pije freskuese, duke futur një monedhë false në një makinë shitëse.[52]

Përcaktimi i momentit të konsumimit të vepres së mashtrimit kompjuterik dhe zbatimit strikt të rregullave të konkurimit ndërmjet vepres kryesore dhe atyre që e shoqërojnë, ose pasojnë merr rëndësi themelore për efekt të kualifikimit ligjor dhe konkurimit të asaj me veprat e tjera penale. Kjo është veçanarisht e rëndësishme në rastet: Punonjësi i një institucioni financiar, i cili, duke ndryshuar sistemin, ose të dhënat, arrin të lëvizë fondet

47 Shih Vendimin e Gjykatës së Kasacionit të Italisë, pen. 26 febbraio 2009, n. 8755, *CED Cassazione* 2009. Nello stesso senso Cass. pen. 5 febbraio 2004, n. 4576, *Giur. it*., 2004..

48 Vendimin e Gjykatës së Kasacionit të Italisë , Sez. II, n. 17748/11, i cili ka mbajtur një qëndirm të kundërt me vendimin Pen., 26 febbraio 2009, n. 8755, CED 243238, në të cilin arsyetohej se "*Krimi i mashtrimit kompjuterik nuk është gjë tjetër veçse një hipotezë specifike e asaj të mashtrimit (omissis)".*

49 Shih Pecorella, C., Commento Art. 640 ter c.p., cit., 6417

50 Duhet të theksohet se nëse subjekti pasiv nuk është sistemi, por një person i cili është shtyrë në gabim përmes përdorimit të mjeteve kompjuterike, psh kur autori arrin të vërë dorë mbi pasurinë e tjetrit, me anë të gënjeshtrës së përdorur në rrjete të ndryshme sociale (si Facebook, Instagram), në të cilat subjekti pasiv, bie në "lajthitje" dhe e dorëzon "vullnetarisht" pasurinë e tij, kualifikimi ligjor duhet të bëhet si *"Mashtrimi"* të parashikuar në nenin 143 të K.Penal.

51 Shih Bartoli, R., La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma, in Dir. inf., 2011, 03, 392 ss.

52 Shih Vendimi i Gjykatës së Kasacionit të Italisë , Sez. VI pen., sez. V, 15.12.2009, n. 14869, in DeJure; in dottrina, v., le ancora attualissime considerazioni svolte da, Manzini, V., Trattato di diritto penale, IX, Torino, 1984,167, nt. 18, nonché 227 e 674

nga një llogari në tjetrën në mënyrë që të mos vihen re[53], apo punonjësi i institucionit të tatimeve, i cili tregon se pagimi i një takse nuk është kryer, ndërsa shumën e përvetëson për vete.[54] Diskutimet lidhur me kualifikimin lidhet shtrihet lidhur me figurat e vepres penale të mashtrimit kompjuterik, vjedhjes duke shpërdoruar detyrën,vjedhjes së bankave dhe arkave të kursimit, shpërdorimit të detyrës, falsifikimit kompjuterik. Pavarësisht ngjashmerive, apo konfuzioneve që krijohen ndërmjet këtyre veprave penale duhet theksuar se këto figura ato nuk kanë relacion specialiteti me njëra tjetren, por në rastet e sipërtreguara janë të qartë elementet e anës objektive dhe subjektive të mashtrimit kompjuterik. Ky konkluzion duhet bazuar edhe në qëndrimin subjektiv të autorit të veprës. Elementi subjektiv nxjerr në pah nëse autori kishte për qëllim të realizojë vjedhjen e bankës si institucion apo ka patur për qëllim të nxjerrë përfitim të padrejtë nëpërmjet përdorimit të aftësive të tij në fushën kompjuterike. Për efekt të kualifikimit ligjor do të ishte e rëndësishme që ligjvënësi të kishte parashikuar si rrethanë renduese shfrytëzimin e cilësisë si operator i sistemit kompjuterik për të kryer vepren penale.[55]

Diskutime të ngjashme ka sjellë në doktrinën e së drejtës dhe në jurisprudencë rasti në të cilin përmes një *skimmeri* (që është ajo pajisje, zakonisht e fshehur në ATM, përmes së cilës mund të kopjohet shiriti magnetik i kartave të pagesës) janë klonuar kartat e pagesave. Më pas duke i përdorur janë realizuar tërheqje cash nga çdo bankomat. Figurat e veprave penale *prima face* janë "*Falsifikimin e letrave me vlerë",* ku përfshihet edhe falsifikimi i kartëkrediteve.[56] dhe mashtrimi kompjuterik. Këto figura të vepres penale nuk konkurojnë ndërmjet tyre, sipas rregullit të konkurimit fiktiv të specialitetit, duke ekzistuar ndërmjet tyre një relacion gjinie/ përgjithshëm dhe një specie/speciale.[57]

---

53 Shih Pecorella, C., Commento Art. 640 ter c.p., cit., 6426 ss

54 Shih Vendimi i Gjykatës së Kasacionit të Italisë , Sez. VI Cass. pen., sez. V, 21.9.2010, n. 40889, in DeJure; nonché Cass. pen., sez. II, 29.9.2010, n. 37127, in DeJure

55 Një parashikim të ngjashëm ka bërë kodi penal Italian, i cili në nenin 640 ter ka parashikuar se: "*ose nëse vepra është kryer me keqpërdorim të cilësisë së sistemit operator... ".*

56 Neni 184 KP "Falsifikimi ose vënia në qarkullim i çeqeve, kambialeve, kartëkrediteve, çekudhëtarëve ose letrave të tjera me vlerë të falsifikuara, dënohet me burgim gjer në pesë vjet. Po kjo vepër, kur kryhet në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda, dënohet me burgim nga tre gjer në dhjetë vjet."

57 Shih Vendimi i Gjykatës së Kasacionit të Italisë, S.U., 28.3.2001, n. 22902, in DeJure; nonché, da ultimo, Cass. pen., sez. II, 10.1.2012, n. 11699, ibidem, e cfr. Cass. pen., sez. II, 15.4.2011, n. 17748, ibidem)

Në jurisprudencën e vendit tonë,[58] është argumentuar se në këtë rast janë konsumuar plotësisht elementët e figurës së veprës penale të "Mashtrimit kompjuterik", parashikuar nga neni 143/b/2 i K.Penal**.** Gjykata ka arsyetuar se:*" ...pasi kanë siguruar karta krediti elektronike "Visa" të falsifikuara kanë ardhur në Shqipëri me qëllim që të mashtronin me këto karta elektronike për të nxjerrë përfitime materiale për veten e tyre.".*

Ndërsa në një rast tjetër identik Gjykata ka vendosur ndryshimin e cilësimit në *"Falsifikim të letrave me vlerë"* me arsyetimin:*" Sa më sipër Gjykata arrin në përfundimin se vepra penale e kryer nga të pandehurit nuk mund të kualifikohet si* **"***Mashtrimi kompjuterik" pasi që të ekzistojë kjo vepër penale duhet që veprimet e të pandehurve të jenë të tilla që nëpërmjet futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike ose me anë të ndërhyrjes në funksionimin e një sistemi kompjuterik ata të kenë pakësuar pasurinë e të dëmtuarit. Në rastin konkret veprimtaria kriminale e të pandehurve është kryer nëpërmjet kartëkrediteve të falsifikuar të cilët parashikohen në mënyrë eksplicite në nenin 184 të K.Penal dhe është element kryesor i kësaj vepre penale. Pra falsifikimi dhe vënia në qarkullim i kartëkrediteve është parashikuar nga ligjvënësi si një vepër penale me vete dhe ka mbrojtje të posaçme për rrjedhojë veprimet kriminale të të pandehurve duhet të kualifikohen në këtë nen." [59]*

Pyetja që lind është: A është karta e kreditit letër me vlerë? Termi "kartëkrediti" i ka krijuar konfuzion, por duhet theksuar se kategoria e letrave me vlerë, kur referon kartëkreditin kupton një lloj letre me vlerë (letërkredit) në kuptim të ligjit përkatës specifik,.[60] Sipas legjislacionit financiar në fuqi letrat me vlerë (ku hyn edhe paraja) konsiderohen të tilla pasi ato kanë një ekuivalencë ekonomike që nuk e kanë letrat e tjera, apo dokumentet e tjera të lëshuara nga institucionet shtetërore apo private. Në këtë grup nuk futen kartat që përmbajnë sisteme kompjuterike të lidhura me sistemin bankar. Nga ana objektive, vepra penale e falsifikimit të letrave me vlerë kryhet me veprime aktive të kundërligjshme, nëpërmjet falsifikimit dhe vënies në qarkullim të letrave me vlerë, duke ndryshuar vlerën (shumën) që ato përfaqësojnë.[61] Ndërsa në kartat kompjuterike të sistemit bankar nuk

58 Shih Vendim nr. 82, datë 27.01.2014, i Gjykatës së Rrethit Gjyqësor Tiranë.

59 Shih Vendim nr. 1689, datë 20.12.2010 i Gjykatës së Rrethit Gjyqësor Tiranë.

60 Neni 2 i Ligjit Nr. 8080, datë.1.3.1996 "Për Letrat me Vlerë" i ndryshuar: "letra borxhi" si instrument që krijon ose konfirmon borxhin që është emëtuar ose propozohet për t'u emëtuar nga një shoqëri që përfshin, në veçanti, letra borxhi me maturim mbi një vit.

61 Shih Ismet Elezi, "E drejta penale e Republikës së Shqipërisë, (Pjesa e posaçme)", fq. 331.

është relevante një mënyrë e tillë të vepruar.

Karta e kreditit është një kartë magnetike që të lejon, nëpërmjet një kodi personal sekret (PIN), tërheqjen e cashit, nxjerrjen e gjendjes së llogarisë dhe nxjerrjen e lëvizjeve të llogarisë pranë sporteleve automatike. Ajo përmban logon e bankës që e ka lëshuar, një element sigurie të paraqitur në formën e një *chip*-i 3 me 5 mm, një numër të dukshëm që është dhe numri i identifikimit të bankës, kohën e skadimit (muajin dhe vitin), një numër ekstra dhe një kod sigurie treshifror (jo të gjitha kartat e kanë këtë kod sigurie).[62] Është pikërisht pajisja e kartës me shirit magnetik, që e kthen kartën e kreditit në vetvete në një sistem kompjuterik.

Për kualifikimin ligjor kuadri ligjor italian paraqet lehtësi për shkak të parashikimit të figurës së vepres penale të *"Përdorimi i padrejtë dhe falsifikimi i instrumenteve të pagesave përveç parave të gatshme",* në nenin 493-ter të Kodit Penal Italian.[63] Dallimi ndërmjet kësaj dhe mashtrimit kompjuterik është evidentuar edhe nga Gjykata e Kasacionit të Italisë[64], e cila arsyeton se: "*.....Krimi i mashtrimit kompjuterik , dhe jo ai i përdorimit të padrejtë të kartave të kreditit, integrohet me sjelljen e personit i cili, duke përdorur një kartë krediti të falsifikuar dhe një kod aksesi të marrë më parë me mashtrim, hyn në mënyrë të paligjshme në sistemin kompjuterik bankar dhe kryen fonde të paligjshme. operacionet e transferimit. Ai integron krimin e përdorimit të padrejtë të kartave të kreditit në përputhje me nenin. 493 ter të Kodit Penal dhe jo ai i mashtrimit kompjuterik, tërheqja e përsëritur e parave në bankomat të një institucioni bankar duke përdorur një mjet magnetik të klonuar.....*".

Gjithashtu në jurisprudencë ka krijuar debate juridike lidhur me cilësimin ligjor, i cili shtrihet ndërmjet figurave të vepres penale të hyrja e pautorizuar kompjuterike,[65] rasti i rimbushjes së telefonisë celulare nga subjekti që është në posedim të fjalëkalimit të sistemit kompjuterik. Gjykata pasi bën

62 Shih Erida Visoçi "Analizë juridiko penale materiale e krimit kompjuterik në këndvështrim teorik, praktik e krahasimor", Shkolla e Magjistrtures, Tirane 2017, fq 49

63 Në këtë nen parashikohet se: "*1. Kushdo për të përfituar prej saj për vete ose për të tjerët, përdor në mënyrë të parregullt, pasi nuk është pronar, karta krediti ose pagese, ose ndonjë dokument tjetër të ngjashëm që mundëson tërheqjen e parave të gatshme ose blerjen e mallrave ose sigurimin e shërbime, ose ndonjë instrument tjetër pagese përveç parave të gatshme, dënohet me burgim nga një deri në pesë vjet dhe me gjobë nga 310 € deri në 1.550 €. I njëjti dënim i nënshtrohet çdo personi që falsifikon ose ndryshon instrumentet ose dokumentet e përmendura në fjalinë e parë me qëllim që të përfitojë prej tij për vete ose të tjerët, ose posedon, transferon ose merr instrumente ose dokumente të tilla me origjinë të paligjshme ose në çdo rast të falsifikuar. ose të ndryshuara, si dhe urdhërpagesat e prodhuara me to.....*".

64 Shih Cass, pen, sezII, 17/06/2019, n.30480

65 Shih nenin 192/b të Kodit Penal.

një analizë të detajuar të veprës penale të mashtrimit kompjuterik dhe të dallimeve me hyrjen e paautorizuar kompjuterike, arsyeton se :*"…..Pasi ajo ka arritur të futet në sistemin EPOS futja e të dhënave kompjuterike është bërë me dashje direkte pasi e pandehura ka parashikuar dhe ka dëshiruar ardhjen e pasojës që është rimbushja e numrave celularë të vendosur prej saj."*[66]

Ky qëndrim është mbajtur edhe nga Gjykata italiane të Kasacionit, e cila ka konsideruar se përbën mashtrim kompjuterik, dhe jo vetëm akses (hyrje) abuzive në një sistem informatik ose telematik, paraqitja në sistemin kompjuterik të *Posta Italiane spa*, përmes përdorimit abuziv të kodeve të aksesit personal të një llogaritari dhe transferimi, në favor të vetes të një shume parash.[67] Në jurisprudencën e saj Gjykata e Kasacionit të Italisë është shprehur se kemi veprën të mashtrimit kompjuterik, në formën e ndërhyrjes pa të drejtë në të dhëna dhe informacione të përmbajtura në një sistem kompjuterik, përveç se të aksesit të paligjshëm në një sistem kompjuterik, kur punonjësi i Agjencisë së të Ardhurave, duke përdorur fjalëkalimin që i është dhënë, ndërhyn në pozitën e taksapaguesit, duke bërë lehtësime pa shkak dhe të pa justifikuara nga evidencat në posedim të zyrës.[68]

Mënyra e shtënies në posedim të kodeve të aksesit shpesh herë përbën veprimin kryesor që konsiston në mashtrim kompjuterik. Gjykata Italiane e Kasacionit ka pranuar se përdorimi abuziv i kodeve kompjuterike të të tretëve (ndërhyrje pa të drejtë), të marrë, apo të shtënë në posedim pa dijeninë apo pa vullnetin e poseduesit të ligjshëm (me çdo mënyrë), është i përshtatshëm për të integruar veprën e mashtrimit kompjuterik kur këto kode janë përdorur për të ndërhyrë pa të drejtë në të dhëna, informacione apo programe të përmbajtura në një sistem kompjuterik apo telematik, me qëllim për të marrë një përfitim të padrejtë për vete apo të tjerët.[69]

Po ashtu, që të konsiderohet se kemi të bëjmë me mashtrim kompjuterik, duhet që personi të përdorë për të hyrë në sistem kode apo fjalëkalime të përftuara në mënyrë të padrejtë apo të marra në mënyrë të paligjshme nga poseduesi legjitim. Këtë qëndrim ka mbajtur Gjykata italiane e Kasacionit, në një rast lidhur me kartat telefonike, ku sipas të cilës integron veprën e përdorimit të paligjshëm të kartave të kreditit apo të pagesës, sjellja e atij që rimbush telefonin celular duke përdorur padrejtësisht kode të lidhura

66 Vendim nr. 995, datë 23.04.2014 i Gjykatës së Shkallës së Parë Tiranë.

67 Shih Corte di Cassazione, Sezione II Penale, Sentenza 24 Febbraio, n.989 .

68 Shih Corte di Cassazione, Sezione II Penale, Sentenza 6 Marzo 2013, n. 13475.

69 Ibid.

me kartat telefonike të kreditit, të marra me mashtrim nga ata që i mbanin në mënyrë legjitime, duke patur parasysh se, karta e parapaguar është një "dokument i ngjashëm" me kartat e kreditit ose të pagesave, që mundëson ofrimin e shërbimeve telefonike.[70] Në këtë rast, Gjykata përjashtoi konfigurimin e veprës së aksesit të paligjshëm në një sistem kompjuterik, të posedimit të paligjshëm të kodeve hyrëse në sistemet kompjuterike dhe të mashtrimit kompjuterik, për shkak se nuk ka pasur sjellje të drejtpërdrejtë për të hyrë në mënyrë të paligjshme në sistemin kompjuterik të kompanisë telefonike dhe as ndryshim të funksionimit të sistemit me qëllim për të marrë një fitim të padrejtë.

Gjykata e Kasacionit të Italisë ka pranuar përputhjen formale midis krimeve të hyrjes së paautorizuar në një sistem kompjuterik dhe atij të mashtrimit kompjuterik, duke arsyetuar se: "*këto janë krime krejtësisht të ndryshme, e dyta prej të cilave postulon domosdoshmërisht manipulimin e sistemit, një element përbërës jo i nevojshëm për përfundimin e së parës: ndryshimi midis dy hipotezave kriminale rrjedh edhe nga diversiteti i të mirave juridike të mbrojtura, nga elementi subjektiv dhe nga parashikimi i mundësisë së kryerjes së krimit të aksesit abuziv vetëm për sa i përket sistemeve të mbrojtura, karakteristikë që nuk shfaqet në krimin e mashtrimit kompjuterik (omissis)".*[71].

Koncepti i mashtrimit kompjuterik ka gjetur aplikim gjithashtu në rastin e ofrimit të sinjalit të platformave digjitale nga subjekte që nuk kanë të drejtën e ofrimit të këtij shërbimi.[72] Kolegji Penal i Gjykatës së Lartë ka vlerësuar se vendimi i Gjykatës së Apelit Tiranë është dhënë në zbatim të drejtë të ligjit material penal dhe si i tillë duhet të lihet në fuqi. Sipas këtij Kolegji: "*...Kjo vepër, nga ana objektive, është kryer në formën e ndryshimit të të dhënave kompjuterike, pasi aparati "Dreambox" që ata kanë shitur, funksionon duke përdorur një kartë Smart të abonuar, e cila është në gjendje të dekriptojë "çelësin" dhe më tej lidhet me internetin, duke bërë të mundur ndarjen e "çelësit/kodeve" në të gjitha aparatet e tjerë, të cilët nuk përdorin kartën Smart....."*[73]

Sipas Raportit Vjetor të Vitit 2021 të Prokurorisë së Pergjithshme

70 Shih Corte di Cassazione, Sezione III Penale, Sentenza 31 Luglio 2003, n.32440.

71 Shih Vendimi i Gjykatës së Kasacionit të Italisë , Sez. VI, n. 3067/99, *CP 00, 2990, nt. Aterno e Cuomo*

72 Shih Vendim nr. 870, datë 01.07.2013 i Gjykatës së Shkallës së Parë Tiranë.

73 Shih Vendim nr. 261, datë 02.10.2013 i Kolegjit Penal të Gjykatës së Lartë.

mbi Gjendjen e Kriminalitetit[74], sa i përket vepres penale "Mashtrimit kompjuterik", pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kopmjuterik" për vitin 2021 është 30,74 %, ndërsa për vitin 2020 ka qenë 40,38%. Nga të dhënat statistikore në vitin 2021 vërehet tendenca në rritje prej 12,69 % e procedime e të regjistruara për veprën penale të parashikuar nga neni 143/b i Kodit Penal "Mashtrimi kompjuterik", në krahasim me vitin 2020.

Konkluzione:

- Objekti juridik i mbrojtjes së figurës së mashtrimit kompjuterik ka karakter multifensiv përfshin mbrojtjen e aktiveve/mirave, të kuptuara si grupi i të gjitha atyre burimeve financiare "të paprekshme", (psh, paratë dhe letrat me vlerë të depozituara në një llogari rrjedhëse të një banke, e cila i menaxhon ato nëpërmjet një sistem kompjuterik), që mund të aksesohen edhe nëpërmjet një sistemi kompjuterik, si dhe në mënyrë indirekte, ka si objekt mbrotjeje "funksionimin e rregullt i sistemeve kompjuterike dhe telematike", si dhe "konfidencialitetit që duhet të shoqërojë përdorimin e tyre".
- Mashtrimit kompjuterik ka një strukturë të dyfishtë, mund të konsumohet në mënyrë alternative me anë të ndërhyrjes në funksionimin e një sistemi kompjuterik ose me anë të futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike. Pavarësisht sjelljes alternative inkriminuese **ligjvënësi** nuk është kujdesur qëtë dyja të përfshijnë nocionin e lirë të sjelljes tipike, për të qënë gjithëpërfshirës. Kjo deduktohetnga mungesa e termit"*në çfarëdo mënyre*", kjo do t'i jepte kësaj hipotezë, mos kërkimin e ndonjësjellje specifike.
- Mashtrimi kompjuterik, në lidhje me krimin e mashtrimit, paraqet elemente autonomie të tilla që e bëjnë të pamundur strukturialisht ekzistencën e një marrëdhënie specialiteti midis dy veprave penale. Ai kriminalizon sjelljet e kryera, të pakundërdrejtuara një personi, por, nëpërmjet manipulimit të një sistemi kompjuterik (duke ndryshuar ose ndërhyrë në një sistem kompjuterik ose telematik, apo në të dhëna, informacione apo programe të përdorura prej tyre), mbron të drejtat pasurore, duke përfshirë të gjitha mjetet dhe instrumentet financiare që

74 Shih faqe 168-170 të Raportit Vjetar të vitit 2021.

mund të menaxhohen edhe nëpërmjet kompjuterit, ose internetit,[75]dhe sjell përfitim të një fitimi të padrejtë, duke dëmtuar të tjerët.

- Për efekt të kualifikimit ligjor do të ishte e rëndësishme që ligjvënësi të kishte parashikuar si rrethanë rënduese në këtë nen shfrytëzimin e cilësisë si operator i sistemit kompjuterik për të kryer veprën penale.

Biblografia.

Literature:

- Corrias L., "Informatica e Diritto Penale: elementi per una comparazione con il diritto statunitense", 1987.

Giovanni Modesti, "Il reato di frode informatica" Una rilettura alla luce delle recenti pronunce giurisprudenziali, aksesuar me datë 09.06.2022 në adresën: http://www.apihm.it/pdf/IlReatoDiFrodeInformatica.pdf

Vaccaio D., L'evoluzione del concetto di misura di sicurezza a protezione del sistema informatico alla luce dell'art. 615-ter e del Disciplinare Tecnico; in ëëë.computerlaw.it,; 2022;

Pomante G., Frode informatica, la soluzione arriva dall'art. 640 ter, su www.pomante.com,

Logroscino S. Analisi e considerazioni sul delitto di Frode informatica quale autonoma figura di reato rispetto al delitto di Truffa , ww.diritto.it (2011);

Romani M. e D. Liokopoulos, La globalizzazione telematica. Regolamentazione e normativa nel diritto internazionale e comunitario, ed. Giuffrè, (2009)

Salvatori I., L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cooking, in Rivista Italiana di Diritto e Procedura Penale, (2008)

Ismet Elezi, "E drejta penale e Republikës së Shqipërisë (Pjesa e posaçme)".

Di Stefano Logroscino La frode informatica quale autonoma figura di reato rispetto al delitto di truffa", Pubblicato il 05/01/2012

Mantovani, F., Diritto penale, pt. spec., II, Delitti contro il patrimonio, III

75 Shih Di Stefano Logroscino La frode informatica quale autonoma figura di reato rispetto al delitto di truffa", Pubblicato il 05/01/2012

ed., Padova, 2009.

Pecorella, C., Il diritto penale dell'informatica, rist. con aggiornamento, Padova, 2006,

Mucciarelli, F., Commento all'art. 10 della l. n. 547 del 1993, in Legisl. pen.,1996,

Antolisei, F., Manuale di diritto penale, pt. spec., I, XV ed., Milano, 2008

Pica, G., Internet, in Dig. pen., Aggiornamento, I, Torino, 2007.

Militello, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in *Rivista trimestrale di diritto penale dell'economia,* 1992

Frosini, V., *Il Disegno di legge sulla repressione dei reati informatici*, in *Informatica e documentazione*, 1993, 1 e 2

V. Rombo, *Crimini informatici alla luce dei nuovi approdi legislativi*, on-line su *www.ceasonline.com/it/*.

Fiandaca-Musco, *Dir. Pen. P. s.*, *I delitti contro il patrimonio*, Bologna, 2002;

Pagliaro, *Principi di diritto penale*, *P. s.*, *Delitti contro il patrimonio*, Milano, 2003;

Antolisei, *Manuale di diritto penale, P.s.*, I, Milano, 2002.

Masi, *Frodi informatiche e attività bancaria, in Rivista penale dell'economia,* 1995

Pecorella, C., Commento Art. 640 ter c.p., in Codice penale commentato, Artt. 575-734 bis, a cura di E. Dolcini e G. Marinucci, III ed., Milano, 2011, 6417

S. Destito, G. Dezzani, C. Santoriello, *Il diritto penale delle nuove tecnologie*, Padova, 2007

Di Stefano Logroscino **"**La frode informatica quale autonoma figura di reato rispetto al delitto di truffa", Pubblicato il 05/01/2012

Dello Iacono, *Articolo 640 ter: truffa o furto? La Frode informatica e il «modello 640»*, in *Temi Romana*, 1996. Di orientamento opposto C. PECORELLA, *Diritto penale dell'Informatica,* Padova, 2006

Pecorella, C., Commento Art. 640 ter c.p., cit., 6417

Cadoppi, A.-Veneziani, P., Elementi di diritto penale, II ed., Padova, 2004,

Pecorella, C., Commento Art. 640 ter c.p., cit., 6418

Picotti, L., Reati informatici, in Enc. Giur. Treccani, Torino, 1991, 27

Bartoli, R., La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma, in Dir. inf., 2011, 03, 392 ss.

Legjislacion:

- Rekomandimi nr. R 899 i Komitetit të Ministrave për shtetet anëtare për kriminalitetin kompjuterik, miratuar për Komitetin e Ministrave më 13 shtator 1989
- Ligji nr. 10 023, datë 27.11.2008.
- Konventës "Për krimin në fushën e kibërnitikës"
- Kodit Penal i RSh
- Council of Europe, European Treaty Series, No. 185, Explanatory Report to the Convention on Cybercrime.
- Kodi penal Italian
- Ligji Nr. 8080, datë.1.3.1996 "Për Letrat me Vlerë" i ndryshuar:

Jurisprudencë:

- Cass. Seksioni VI, 4 tetor 1999
- Cass. pen., sez. II, 24.2.2011, n. 9891, in DeJure
- Vendim nr. 995, datë 23.04.2014 i Gjykatës së Shkallës së Parë Tiranë
- Cass. pen., sez. V, 19.3.2010, n. 27135, in DeJure,
- Cass, pen., sez. I, 24.2.2012, n. 11473, in DeJure
- Cass, pen., sez. V, 19.3.2010, n. 27135, in DeJure
- Cass, pen., pen. 26 febbraio 2009, n. 8755, CED Cassazione 2009. Nello stesso senso Cass. pen. 5 febbraio 2004, n. 4576, Giur. it., 2004..
- Cass, pen , Sez. II, n. 17748/11,
- Cass, pen., sez 26 febbraio 2009, n. 8755, CED 243238,
- Vendimi i Gjykatës së Kasacionit të Italisë , Sez. VI, n. 3067/99, CP 00, 2990, nt. Aterno e Cuomo

- Cass, pen, Sez. VI pen., sez. V, 15.12.2009, n. 14869, in DeJure;
- Cass, pen, sez. V, 21.9.2010, n. 40889, in DeJure;
- Cass. pen., sez. II, 29.9.2010, n. 37127, in DeJure
- Cass, pena, S.U., 28.3.2001, n. 22902, in DeJure;
- Cass. pen., sez. II, 10.1.2012, n. 11699,
- Cass. pen., sez. II, 15.4.2011, n. 17748, ibidem)
- Vendimi nr. 82, datë 27.01.2014, i Gjykatës së Rrethit Gjyqësor Tiranë.
- Vendimi nr. 1689, datë 20.12.2010 i Gjykatës së Rrethit Gjyqësor Tiranë.
- Vendimi nr. 995, datë 23.04.2014 i Gjykatës së Shkallës së Parë Tiranë.
- Corte di Cassazione, Sezione II Penale, Sentenza 24 Febbraio, n.989 .
- Corte di Cassazione, Sezione II Penale, Sentenza 6 Marzo 2013, n. 13475.
- Corte di Cassazione, Sezione III Penale, Sentenza 31 Luglio 2003, n.32440.
- Vendimi nr. 870, datë 01.07.2013 i Gjykatës së Shkallës së Parë Tiranë.
- Vendimi nr. 261, datë 02.10.2013 i Kolegjit Penal të Gjykatës së Lartë.

INTERNATIONAL CORRUPTION: CHARACTERISTICS AND IMPORTANCE OF THE INTERSTATE DISCIPLINE.

AVV. PROF. ERSI BOZHEKU[1]

I. Introduction

As is known, international corruption is integrated in cases in which money or other benefits are given to a foreign public official to obtain an act for the benefit of an entity that has its headquarters or operates in a State other than that of the legal system to which it belongs. of the public official.

This phenomenon has become increasingly important with the progressive enlargement of the market. In fact, the opportunities for contact with public officials of States other than the one in which the companies are established or have their own operational headquarters have multiplied.

With the growth of the phenomenon, distorting effects of international competition have arisen which these practices have entailed, in connection with the different treatment reserved, in the country of origin of the entity, to the corrupt practices of foreign public officials.

In particular, those companies established as entities in countries where international corruption was tolerated or even facilitated were in fact favored, compared to countries where such practices involved sanctions not only for the natural persons who had carried them out, but also for legal entities and companies that had benefited from it.

From the need to avoid such distorting effects, therefore, the urgency, felt more internationally than of individual states, arose to regulate sanctioning the phenomenon of bribery of foreign public officials.

1 Lawyer at the bar of Rome. Associate Professor of Criminal Law. Executive Director of the "CESIAL - Italian-Albanian Studies, Higher Education and Research Center of the CEMAS "Sapienza" University of Rome.

The intervention held at the Conference aimed at clarifying the interpretative problems that arise in relation to the crime of international corruption and in relation to the difficulties of ascertaining it.

II. The discipline of international corruption and the Italian legal system

The phenomenon of international corruption is increasingly present in the globalized world of the economy. It is important to react to it for two main reasons: the first is that the corruption alters the mechanism of competition incentives on world markets, and the formation of adequate and common legal protection is necessary to ensure equality competition between companies on world markets; it is also necessary to help countries in Way of Development in their economic and social growth, because corruption constitutes first of all a strong distortion of the allocation of resources, diverting above all those that could be destined for development.

The OECD Convention of 17 December 1997 on Combating Bribery of Public foreign officers in international business operations fight corruption international by requiring member states to consider individuals a crime e legal for bribing foreign officials to obtain undue advantages in international trading.

The rules implementing the Convention in Italy are fully effective from 4 July 2001.

The Italian legal system introduced, from the point of view of the corruption of persons, art. 322bis of the Italian Criminal Code which punishes embezzlement, extortion, corruption and incitement to bribery of members of European Community bodies and official of the European Communities and foreign states, applying various criminal offenses [art. 314 e 316, from 317 to 320 and 322] to officials of the European Communities and public officials and persons in charge of public service in the Member States of the European Union.

III. The criminal liability of companies

But the major novelty of the implementation of the OECD Convention in Italy is the obligation toalso directly prosecute legal persons responsible for corruption. There criminal liability of legal persons, introduced by Legislative Decree 231 of 2001, provides that an entity (including partnerships and

corporations) is responsible for bribery offenses committed in its interest or to the advantage of the persons they cover functions of representation, administration, management or control (including de facto), or controlled by and dependent on them.

The rule concerns not only legal persons of Italian law, but also entities, companies and enterprises having their head office in Italy, which they also respond in relation to the offense committed abroad "provided that they do not the State of the place where the offense was committed is to proceed.

The company can avoid be sanctioned if the management body has adopted and effectively implemented, before the commission of the fact, suitable organizational and management models a prevent crimes of the kind that occurred, and has been entrusted to a body independent of the body the task of supervising the functioning and observance of the models this has done so effectively.

The liability of the entity and its prosecution are independent of that of the accused: they can therefore coexist.

Italian legislation also provides for the preparation of appropriate codes of behavior as a guide for business organization models: it is a means of prevention of corruption through the involvement of civil society and trade associations.

In cases where the infringement is ascertained, the company is liable to administrative pecuniary sanctions and, in the most serious cases, also to sanctions prohibiting the exercise of the activity, the suspension or revocation of authorizations, the prohibition of contracting with the public administration, exclusion from subsidies, loans or contributions, the ban on advertising goods or services.

However, the novelty of the law did not play in favor of its immediate practical application, which in Italy did not have great success in the first years of application.

With reference to the proceedings for international corruption initiated in Italy starting from the entry into force of the OECD Convention, until 31.12.2015, there are 57 investigations initiated during the entire reference period; of these, 18 proceedings are still in the investigation phase, 9 in the trial phase, 26 proceedings are concluded with only one conviction which has become res judicata and one non-definitive sentence.

These data show that, although international corruption constitutes the historical matrix of the very introduction of the Italian legislation on the

subject of criminal liability for legal persons, up to now the Legislative Decree 231/2001 has mainly received application for offenses dependent on crimes of corruption of natural persons, in this case public officials belonging to the legal system of the Italian State.

IV. The importance of the interstate discipline

In conclusion, it is evident that both in the hypothesis of international corruption contested against individuals and in the hypothesis of offenses contested against companies, the existence of a more homogeneous discipline in the various countries involved is extremely important.

Coordination between the disciplines of the various countries is important at first when it is necessary to ascertain corruption offenses and at a later time when the sanctions are applied.

Therefore, the future development of close collaboration between the investigating authorities of the various countries and, even before that, at the legislative level, an ever higher harmonization of the disciplines incriminating international corruption in individual countries can only be desirable.

ORGANIZED CRIME AND THE USE OF TECHNOLOGY FOR COMMUNICATION PURPOSES

RENIS SHESHI[1]
renissheshi@yahoo.com

ALBAN NAKO[2]
alban.nako@gmail.com

Abstract

The internet 2.0 is a worldwide phenomenon, technological advances have deeply impacted our society providing new tools to enhance the human experience and capabilities, today everyone is online. Communication is one of the basic requirements for a society and with the advent of a new age in communication technology, people connect with ease from every corner of the globe. Communication is an essential tool to sustain the growth, therefore secure communication is quintessential when everyone is watching. This has created a new range of possibilities completely unimaginable before. But as with all and any technological advances, there lies a possibility of threat of abuse. Organized crime relies upon faster and secure communication to guarantee survival against other criminal entities and law enforcement agencies.

In this paper, we extrapolate the idea that ordinary social media tools are used extensively by organized crime to further their agenda and communicate among peers. Social platforms that are popular offer a cheap and sustainable tool for every to "blend in" among other users. Being anonymous behind a screen offers a certain level of protection but further level of security measures is added like proxy IP addresses and using encrypted systems. In a

complex online world, the most effective tool of communication is by mixing online and offline techniques to guarantee total anonymousity.

Criminal organization offer also a specialized market for encrypted communication apps. Special communication apps heavily based on encryption provide a perfect tool for criminal organizations to communicate undetected by law enforcement agencies. That is why cracking these apps could deal a heavy blow to criminal activity and provide law enforcement agencies with ample proof for the successful prosecution of the members.

The final part of this paper is focused on the detection and decryption of the communication techniques and various apps used by criminal organizations.

***Keywords**: Criminal organizations, communication apps, encryption, law enforcement.*

1. Hyrje

Zhvillimet shkencore dhe teknologjike kanë ndryshuar në mënyrë dinamike dhe rrënjësore botën njerëzore dhe sot interneti dhe teknologjia janë të pranishëm në pothuajse çdo aspekt të jetës duke udhëhequr mënyrën sesi njerëzit jetojnë dhe marrin vendime. Zhvillimi i vrullshëm i teknologjisë dhe rritja e numrit të përdoruesve ka ndikuar në mënyrën sesi shoqëria njerëzore komunikon duke sendërtuar mekanizma të shpejtë dhe të sigurt (Coe, 2015).

Por edhe në një botë ku të gjithë janë të lidhur në kohë reale me njëri tjetrin, dëshira për privatësi dhe komunikime të sigurta vazhdon të ekzistojë. Për rrjedhojë metodat e sigurta të komunikimit janë tejet të rëndësishme, veçanërisht kur bëhet fjalë për shkëmbimin e informacioneve, të cilat vetë për nga natyra e tyre nuk mund të jenë publike *(sekrete shtetërore, informacione që ekspozojnë aspekte të jetës private)*.

Teknologjia e informacionit ofron në mënyrë vazhduese teknika, metoda dhe mjete të cilat kur përdoren në mënyrën e duhur, brenda rregullave etike dhe ligjore, prodhon efekte pozitive për shoqëritë njerëzore. Popullariteti i përdoruesve të mjeteve të teknologjisë së informacionit ka ndikuar drejtpërsëdrejti në joshjen e krimit të organizuar që të përdori këtë teknologji për arritjen e qëllimeve kriminale.

Rrezikshmëria që paraqet krimi i organizuar në një shoqëri të lirë dhe demokratike është botërisht e njohur. Sigurimi i qetësisë së çdo individi, dhe në një koncept më të gjerë i të gjithë shoqërisë, është detyrë e shtetit dhe një nga detyrat më të rëndësishme të tij, sepse me kryerjen e akteve kriminale dhunohen jo vetëm të drejtat dhe liritë e njeriut, por dhe vlera të njohura dhe të mbrojtura nga Kushtetuta.

Kështu ekzistenca e metodave të shpejta, të lira e të sigurta të komunikimit, ofron avantazhe të shumta për krimin e organizuar. Organizatat dhe grupet e strukturuara kriminale, kanë nevojë për mënyra të sigurta komunikimi ndërmjet anëtarëve me qëllim zhvillimin e veprimtarisë së tyre. Për këto qëllime, mund të shërbejnë aplikacione të specializuara të cilësuara si 'dark networks' që janë të fshehta dhe të paligjshme (Raab & Milward, 2003) por dhe rrjetet sociale. Krijimi i *'networks'* (rrjeteve)[1] kriminale u mundëson këtyre grupeve të tejkalojnë problemet logjistike dhe të mobilizimit dhe në të njëjtën kohë të komunikojnë me një numër të madh njerëzish në distanca të mëdha (Everton, 2013; Gerdes, 2015).

1 Përkthim i autorëve

2. Përdorimi i rrjeteve sociale nga organizatat kriminale

Rrjetet sociale ofrojnë një mënyrë të lirë dhe të thjeshtë komunikimi në mënyrë anonime dhe të sigurt, i gjithë ky proces dinamik dhe organik garantohet nga nevoja e vazhduese për të evoluar platformën sociale me qëllim garantimin e cilësisë së komunikimit të përdoruesve por mbi të gjitha garantimin e mbijetesës përkundrejt platformave të reja që krijohen rishtazi (Dijck, 2013). Një nga opsionet e reja më të përhapura që po ofrohet së fundmi nga shumë rrjete sociale të tilla si 'Facebook.com', 'Twitter.com', 'Instagram.com', 'Snapchat.com' etj., është mundësia e fshirjes së mesazheve pas leximit të tyre nga marrësi (Mercado, 2021).

Një opsion i tillë mund ti shërbejë personave të përfshirë në veprimtari kriminale për shkak se bisedat e zhvilluara në këtë mënyrë nuk ruhen në asnjë vend për dokumentim dhe përdorim të mëvonshëm nga organet ligj zbatuese (Morselli C. , 2009). Gjithashtu dhe interceptimi i këtyre bisedave shfaq vështirësi, pasi rrjetet e famshme sociale përgjithësisht reklamojnë privatësinë e komunikimeve ndërmjet përdoruesve të tyre. Për rrjedhojë krijuesit e tyre përpiqen shumë për të ofruar komunikime sa më të sigurta e të vështira për tu çkoduar. (shembull Whatsapp).

Konstatohet që grupet kriminale dhe rrjetet kriminale, kryesisht, shfaqin tendenca sofistikimi për të shmangur hetimin apo ndjekjen penale nga agjencitë ligj zbatuese. Përdorimi i nofkave, i gjuhës së koduar si dhe shmangia e komunikimeve të drejtpërdrejta të anëtarëve kryesorë të rrjetit apo grupit kriminal, janë disa nga mënyrat që manifestohet përshtatshmëria e sjelljes së këtyre grupimeve. Duke pasur në konsideratë, që përgjimet telefonike shërbejnë si indicje gjyqësore, konstatohet që këto komunikime synohen të shmangen në maksimum duke përfituar nga komoditeti që ofrojnë teknologjitë e komunikimit që krijohen në vazhdimësi.

Megjithatë në rastin e krimit të organizuar, grupeve i duhet të mbajnë struktura të qëndrueshme me shumë anëtare dhe për rrjedhojë dhe metoda të qëndrueshme të komunikimit. Mbajtja e një rrjeti me përdorues me identitete të rreme në një rrjet social, shfaq rrezikun e infiltrimit të rrjetit. Një prej përdoruesve mund të jetë agjent i organeve policore dhe bëhet e vështirë për anëtarët e grupit kriminal ta identifikojnë atë sa kohë që identiteti i tyre mbahet i fshehtë. Një nivel më i lartë i sigurisë së komunikimit mund të arrihet nëpërmjet përdorimit të VPN (virtual private network) *(aplikacione që krijojnë adresa virtuale joreale si dhe shfaqin vendndodhje joreale të përdoruesit)* por dhe sistemeve të enkriptuara.

Sistemi VPN më i famshëm sot në botë është "The TOR Project"

i sendërtuar si një mjet për të luftuar regjimet arbitrare që synojnë të kufizojnë internetin në shtetet e tyre, si në rastin e Kinës apo Koresë së Veriut (Collier, 2020). Pavarësisht qëllimit pse është krijuar, "TOR" është një nga mekanizmat kryesorë të "Dark Web" (interneti i errët). Duhet ta përfytyrojmë internetin si një ajsberg, ku maja e dukshme ajsbergut janë faqet e indeksuar p.sh në google, mediat sociale, aktivitetet që ne kryejmë rëndom kur përdorim një celular apo një kompjuter e cila në tërësinë e saj është vetëm 19 TB, ndërsa dark web-in duhet të përfytyrojmë pjesën që nuk duhet të ajsbergut e cila përdoret nga një numër shumë i kufizuar personat në botë por që krijon një trafik prej 7500 TB. Raporti i zhdrejtë midis internetit dhe dark web-it, lidhet kryesisht me aktivitetin kriminal që kryhet në këtë hapësirë virtuale.

Organizatat kriminale kombinojnë teknika "black hat" (që kanë të bëjnë me thyerjen e rregullave etike të përdorimit të internetit) me metoda "offline" të ritualeve/kodeve të brendshme të komunikimit ndërmjet individëve të organizatës. Kriptimi paraprak i mesazheve ndërmjet anëtarëve duke u transmetuar në kanale të "dark web" kombinuar dhe me përdorimin e një VPN, ofron garanci të shtuar për organizatat kriminale dhe agjendën e tyre.

Organizatat dhe grupet kriminale i përdorin rrjetet sociale jo vetëm për të komunikuar së brendshmi pra nëpërmjet anëtarëve të tyre por dhe si një mjet komunikimi tejet efikas me botën e jashtme.

Kohët e sotme disa organizata kriminale po përdorin rrjetet sociale për të reklamuar mënyrën e jetesës së anëtarëve të tyre si dhe për të projektuar një imazh force. Reklamimi i mënyrës së jetesës i shërben më së miri qëllimit të rekrutimit të anëtarëve të rinj duke treguar një imazh të një stili jetese luksoze të krijuar si pasojë e përfshirjes në veprimtari kriminale.

Sipas studimit të (Morselli & Décary-Hétu, 2013), nuk ka prova të plota që vizitorët e faqeve apo shikuesit e postimeve që reklamojnë mënyrën e jetesës kriminale po manipulohen, nga ana e anëtarëve të grupeve kriminale për t'ju bashkuar atyre. Por nga ana tjetër shikuesit apo vizitorët e këtyre faqeve po tregojnë kuriozitet dhe ndërmjet tyre që ndajnë komente dhe opinione, ka shenja të qarta që tregojnë mbështetje për këtë mënyrë jetese.

Këto rrjete sociale kanë krijuar mundësi të reja për anëtarët e grupeve kriminale që të ndërveprojnë me numra të mëdhenj njerëzish, duke i ekspozuar ata ndaj mënyrës së tyre të jetesës. Diçka e tillë do të ishte e pamundur të realizohej nëpërmjet ndërveprimit fizik (Morselli & Décary-Hétu, 2013).

Nëpërmjet rrjeteve sociale, organizatat kriminale gjithashtu tregojnë dhe influencën e tyre nëpërmjet numrit të mbështetësve. Një numër i madh i mbështetësve e bën më të vështirë punën e autoriteteve duke vështirësuar gjetjen e bashkëpunëtorëve apo informatorëve apo dhe shkurajuar zyrtarët nga ndërmarrja e aksioneve të caktuara kundër këtyre grupeve (Quirk & Campbell, 2015).

Autoritetet e SHBA dhe Kanadasë po përdorin termin "cyberbanging" për t'ju referuar fenomenit të tregimit të forcës kriminale, rekrutimit të anëtarëve apo dhe të veprimit në mënyrë direkte kundër armiqve, nga ana e organizatave kriminale, në rrjetet sociale (Gastelum-Felix, 2014).

3. Monitorimi i rrjeteve sociale nga organet ligj zbatuese si mënyrë për mbledhjen e informacionit për veprimtaritë kriminale

Interceptimi dhe analizimi i komunikimeve nëpërmjet rrjeteve sociale i grupeve kriminale ofron avantazhe të shumta për autoritetet ligj zbatuese. Tejet të dobishme për autoritetet ligj zbatuese shfaqen dhe komunikimet e jashtme, ato reklamuese, nëpërmjet postimeve publike që anëtarët e grupeve kriminale realizojnë.

Postime që reklamojnë një stil jetese luksoz i cili nuk i përgjigjet të ardhurave reale të deklaruara të një individi mund të shërbejnë si shkas për të krijuar dyshime mbi përfshirjen e tij n aktivitete kriminale. Nga ana tjetër postime që tregojnë lëndë narkotike, armatime etj., të cilat nuk janë të rralla në rastin e anëtarëve të grupeve kriminale (Gastelum-Felix, 2014), mund të shërbejnë si indicje apo dhe si prova të përfshirjes në veprimtari kriminale.

Komunikimi i jashtëm, lehtësisht i interceptueshëm i organizatave kriminale nëpërmjet rrjeteve sociale, mund të përdoret dhe më tej nga ana e autoriteteve ligj zbatuese.

Në vitin 2016 u konkludua një projekt i quajtur ePOOLICE *(early Pursuit against Organised crime using environmental scanning, the Law and IntelligenCE systems),* (Ndjekja e hershme e krimit të organizuar duke përdorur, skanimin mjedisor, ligjin dhe sistemet inteligjente)[2]. Ky projekt synonte të zhvillonte një sistem prototip të skanimit mjedisor, i cili do të integronte shumë komponentë teknik me qëllim filtrimin semantik të informacionit nga interneti dhe mediat sociale për të identifikuar

2 Përkthim i autorëve.

informacionin që mund të përbënte të ashtuquajturat *sinjale të dobëta* të krimit të organizuar (Pastor & Larsen, 2017).

Koncepti i sinjaleve të dobëta është marrë nga Shërbimet e Inteligjencës Kriminale të Kanadasë (CISC) të cilët i klasifikojnë treguesit e krimit të organizuar në tregues primarë dhe sekondarë. Sinjalet e dobëta në vetvete nuk mund të shërbejnë si tregues të fenomeneve të krimit të organizuar por kur grupohen sipas kritereve të caktuar, vendndodhjes gjeografike etj., ata kthehen në tregues të prezencës së një veprimtarie kriminale të caktuar (Criminal Intelligence Service Canada (CISC), 2017).

Nëpërmjet mbledhjes dhe analizës automatike të të dhënave projekti synonte të identifikonte në një moment të hershëm formacionet e krimit të organizuar përpara se këto grupime të zhvilloheshin n sisteme më të avancuara e rezistente kriminale (Pastor & Larsen, 2017).

Të dyja format e komunikimit të brendshme dhe të jashtme që realizojnë grupet kriminale nëpërmjet rrjeteve sociale ofrojnë mundësi të shumta për autoritetet ligj zbatuese që të identifikojnë ekzistencën dhe veprimtarinë e grupeve kriminale por dhe të mbledhin informacion mbi anëtarësinë e këtyre grupeve.

Për rrjedhojë monitorimi i këtyre rrjeteve qoftë nëpërmjet metodave konvencionale të vizitimit apo shikimit të postimeve të personave që dyshohen për përfshirjen në veprimtari kriminale, qoftë nëpërmjet metodave tejet të avancuara si ePOOLICE është i nevojshëm për të shfrytëzuar dizavantazhin kryesor që paraqesin këto rrjete për krimin e organizuar, të qënurit i hapur për publikun.

Rëndësia tejet e madhe e mbledhjes së informacionit nga rrjete sociale madje ka shtyrë në konceptimin e një domeni të ri të mbledhjes së të dhënave, ato të 'Social Media Intelligence' (SOCMINT). Ky term është përdorur për herë të parë në një punim të shkruar nga Sir David Omand, Jamie Bartlett dhe Carl Miller në një think-tank me bazë në Londër.

Sipas autorëve në një epokë ku rrjetet sociale janë të kudondodhura, është përgjegjësia e komunitetit të sigurisë që të bëjë SOCMINT pjesë të kuadrit kombëtar të inteligjencës (Omad, Barlett, & Miller, 2012), por vetëm nëse kalohen dy teste të rëndësishme. I pari që informacioni i përftuar të bazohet në një themel të fortë metodologjik të mbledhjes, provimit, verifikimit, kuptimit dhe aplikimit. I dyti, që të mund të menaxhohet rreziku moral që përmban një aplikim i tillë.

4. Përdorimi i aplikacioneve të specializuara të komunikimit elektronik

Organizatat kriminale ofrojnë gjithashtu një treg të specializuar për aplikacione komunikimi të enkriptuar (Soudijn, Vermeulen, & van der Lesst, 2022). Aplikacione të tilla i mundësojnë organizatave mjete perfekte për komunikime të fshehta dhe të sigurta ndërmjet anëtarëve (Shillito, 2019). Si shembull sjellim aplikacionet EncroChat dhe Sky ECC.

Sky ECC ishte një aplikacion për dërgimin e mesazheve të enkriptuara, krijuar nga një shoqëri kanadeze Sky Global. Ky aplikacion ofronte komunikime anonime, të sigurta dhe të pagjurmueshme ndërmjet përdoruesve të tij. Fillimisht u krijua për platformën BlackBerry ndërsa më pas u zgjerua për përdorim dhe nga platforma të tjera.

Kompania gjithashtu modifikonte telefona Nokia, Apple dhe Blackberry, të cilët i çaktivizonte kamerat, mikrofonat dhe GPS. Mesazhet e tyre ishin të enkriptuara dhe fshihen automatikisht pas 30 sekondash. Nëse telefoni të cilit i dërgohej ishte jashtë mbulimit të rrjetit, mesazhi ruhej deri në 48 orë më pas fshihej gjithashtu automatikisht (Spadafora, 2021).

Telefonat ishin të pajisur me një password, i cili nëse futej nga përdoruesi, bënte që pajisja të fshinte të gjithë përmbajtjen e saj.

Më 9 mars të vitit 2021, rreth 1600 oficerë të policisë Belge, arrestuan 48 persona dhe sekuestruan 1.2 milion euro si dhe 17 ton kokainë në rreth 200 kontrolle të befasishme të koordinuara. Pjesë e të arrestuarve ishin avokatë, oficerë policie, një punonjës prokurorie, nëpunës civil (Chini, 2021).

Ky operacion u bë i mundur falë ç'kodimit të rrjetit të aplikacionit Sky ECC nga autoritetet holandeze dhe belge. Këto autoritete kishin aksesuar rrjetin që më datë 15 shkurt 2021 duke interceptuar mbi 1 miliard mesazhe.

Sipas raporteve të policisë belge, përdoruesit e këtij aplikacioni kishin besim të tillë tek ai sa që dërgonin foto torturash, urdhra për ekzekutimin e personave, si dhe informacione të tjera të brendshme lirisht ndërmjet tyre (Boffey, 2021).

Një tjetër aplikacion me mënyrë funksionimi të ngjashme është dhe EncroChat. Shoqëria EncroChat ofronte gjithashtu telefona celularë të cilëve ju ishte çaktivizuar paraprakisht kamera, mikrofoni dhe GPS si dhe ishte instaluar një sistem operativ i veçantë i prodhuar nga shoqëria në fjalë. Telefonat kishin të instaluar një aplikacion për komunikimin e enkriptuar të quajtur EncroChat.

Në vitin 2017, forcat policore franceze (Xhandarmëria kombëtare) zbuluan për ekzistencën dhe përdorimin e aplikacionit nga krimi i organizuar. Megjithatë në atë kohë ishte e pamundur për ta ç'koduar atë dhe për të thyer enkriptimin e telefonave të cilat fshinin të gjitha të dhënat e tyre sapo diktonin një ndërhyrje të mundshme.

Pas marrjes së fondeve nga Bashkimi Evropian në vitin 2019, hetimet u përshpejtuan ndjeshëm. Në janar të vitit 2020, gjykata e Lilit, Francë autorizoi infiltrimin e serverëve të EncroChat. Policia franceze së bashku me policinë holandeze dhe nën mbështetjen e Europol-it, formuan një ekip të përbashkët të hetimit dhe arritën të interceptojnë dhe ç'kodojnë mesazhet pas instalimit të një virusi në serverat e EncroChat në Francë (Cox, 2020). Në maj të vitit 2020, organet ligjzbatuese çaktivizuan opsionin e fshirjes së të dhënave në shumë pajisje. Kompania u përpoq të bënte një përditësim të softuerit me qëllim adresimin e këtij problemi por pa sukses.

Operacioni kulmoi me arrestimin e mbi 100 personave të dyshuar dhe konfiskimin e sasive të mëdha të lëndëve narkotike, armëve, parave, automjeteve të vjedhura etj., në Holandë. Arrestime u bënë gjithashtu në Suedi dhe në Francë.

Në Mbretërinë e Bashkuar filloi operacioni 'Venetic', si rezultat i infiltrimit të rrjetit të EncroChat në Mbretërinë e Bashkuar nga ana e Agjencisë Kombëtare të Krimit (NCA). 746 persona u arrestuan dhe shuma të mëdha parash, armësh dhe lëndësh narkotike u konfiskuan.

Dy shembujt e mësipërm ilustrojnë si shkallën e gjerë të përdorimit të aplikacioneve për komunikime të sigurta nga ana e krimit të organizuar ashtu dhe benefitet që ofron ç'kodimi i tyre dhe interceptimi i bisedave për goditjen e organizatave dhe grupeve kriminale.

5. Gjurmimi dhe zbulimi nga organet ligj zbatuese

Ndërsa avancimet teknologjike ofrojnë lehtësira e mundësi të shtuara për organizatat kriminale pavarësisht ndryshimeve të ngadalta ligjore për të reflektuar realitetin virtual dhe mundësitë financiare për t'ju përshtatur këtij realiteti, (Angelini & Gibson, 2007), po këto ndryshime të vrullshme ofrojnë gjithashtu dhe mundësi të shumta për goditjen e këtyre organizatave nga organet ligjzbatuese.

Avantazhet teknologjike nuk janë të fundme por një proces vazhdues dhe organizatat kriminale duke pasur një përparësi në teknologji shpeshherë e

shohin këtë përparësi si përfundimtare dhe shfaqen të sigurt në fshehtësinë komunikimeve të tyre, duke komunikuar në mënyrë të hapur, të shpeshtë, pa fjalë të koduara dhe në përgjithësi pa marrë masa të tjera mbrojtjeje nga zbulimi.

Për këto arsye, interceptimi i komunikimeve dhe ç'kodimi i tyre bën të mundur ekspozimin e plotë të organizatës, anëtarëve të saj si dhe veprimtarisë kriminale të ushtruar prej saj (Etges & Sutcliffe, 2010).

Ndërsa metoda më efikase për të realizuar komunikime të sigurta nga organizatat kriminale është një miksim i elementëve online dhe offline siç u parashtrua dhe gjatë punimit, po ashtu dhe metoda më efikase për zbulimin e tyre, është një kombinim i metodave të infiltrimit apo kontrolleve dhe teknikës kompjuterike (ç'kodimit, përdorimit të viruseve etj.).

Hapi i parë në ç'kodimin e mjeteve të komunikimit të një organizate kriminale është evidentimi i përdorimit të mjetit prej anëtarëve të saj. Infiltrimi i grupeve kriminale dhe në mungesë të tij, gjetja e telefonave apo pajisjeve të tjera teknologjike në mënyrë rastësore gjatë kontrolleve, çojnë në zbulimin e ekzistencës së këtyre aplikacioneve si dhe faktit të përdorimit të tyre nga organizatat kriminale (Hadjimatheou, 2017).

Këto të dhëna mund të përdoren më pas për marrjen e autorizimit nga ana e gjykatës apo prokurorisë për përdorimin e teknikave kompjuterike me qëllim ç'kodimin e aplikacioneve dhe interceptimin e bisedave. Teknikat kompjuterike nga ana e tyre janë të kushtueshme dhe kërkojnë personel tejet të specializuar të kombinuar me mjetet të teknologjisë së fundit. Përftimi i aseteve financiare të mjaftueshme për operacione të tilla të teknologjisë së informacionet paraqet sfidë dhe për organet ligjzbatuese të vendeve të zhvilluara siç dhe u demonstrua në rastin e operacionit për ç'kodimin e aplikacionit EncroChat.

Për këtë arsye, është e nevojshme që autoriteteve ligjzbatuese të ngarkuara me operacione të tilla të jenë ta pajisura me fondet e nevojshme për realizimin e tyre. Rezultatet që arrihen nga suksesi i interceptimit dhe ç'kodimit të aplikacioneve të kësaj natyre përgjithësisht e justifikojnë tërësisht koston qoftë për sa i përket rëndësisë së goditjes së krimit të organizuar, qoftë dhe për sa i përket vlerës së aseteve kriminale që konfiskohen në përfundimin e suksesshëm të operacioneve të kësaj natyre.

Interceptimi i bisedave bën të mundur më pas mbledhjen e të dhënave mbi anëtarët e organizatës si dhe veprimet kriminale në të cilat ata janë të angazhuar.

Të dhënat të mbledhura në sasi të mjaftueshme, i mundësojnë organeve ligj zbatuese të ndërmarrin operacionet të arrestimit dhe ndalimit të anëtarëve të organizatës si dhe ti procedojnë në mënyrë të suksesshme më pas.

Dilema taktike që shfaqet, në rastet kur organet ligj zbatuese arrijnë të thyejnë një mënyrë të koduar komunikimi online është midis ndërhyrjes së menjëhershme për të ndaluar krimet në vazhdim dhe lejimit taktik të aktivitetit kriminal me qëllim krijimin e një tabloje më të qartë të të gjithë pjesëmarrësve në këtë veprimtari. Dilema tradicionale midis të fituarit të një luftë apo një beteje, e shfaqur në momente të tilla historike si momenti kur britanikët dekriptuan makinerinë e famshme "enigma" të gjermanëve, rishfaqet në kohën moderne në dilemën e organeve ligj zbatuese në eliminimin e grupeve kriminale. Dekriptimi i komunikimit mund të çojnë në goditjen e të gjithë organizatës ose grupit dhe në dënimin e anëtarëve të saj, por vonesat e shumta përpara ndërmarrjes së aksionit i japin kohë programuesve të aplikacioneve që të zbulojnë pikat e dobëta dhe ti adresojnë ato, apo grupeve kriminale që të zbulojnë faktin e dekriptimit e të ndërpresin përdorimin e tij.

6. Konkluzione

Ndryshimet teknologjike janë të vrullshme dhe synojnë përmirësimin e eksperiencës njerëzore, por shpeshherë këto ndryshime mbartin rrezikun që këto metoda dhe sisteme të keqpërdoren në dobi të qëllimit kriminal. Studimi i metodave aktuale të komunikimit të përdorura nga krimi i organizuar është një mjet shumë efikas në luftën kundër krimit të organizuar, i cili shfrytëzon maksimalisht avancimet teknologjike për ushtrimin e veprimtarisë kriminale.

Me qëllim rritjen e efikasitetit në luftën kundër kriminalitetit të organizuar që përdor në mënyrë aktive teknologjinë e informacionit, nevojitet krijimi dhe përditësimi adekuat i infrastrukturës ligjore dhe teknike nga organet ligj zbatuese. Rritja e kapaciteteve të burimeve njerëzore që hetojnë krimin e organizuar mbetet imperative, duke imponuar që këto njësi të hetimit të krimit të kenë karakter hibrid si përsa i përket aftësisë hetuese e policore ashtu dhe të teknologjisë së informacionit. Organet ligjzbatuese duhet gjithashtu të pajisen me asetet financiare të nevojshme për ndërmarrjen e operacioneve që kërkojnë përdorimin e teknologjisë së lartë. Operacione të tilla vetë për nga natyra e tyre, për shkak të pajisjeve dhe personelit të specializuar vijnë me një kosto të lartë financiare, kosto e cila është e justifikueshme për shkak të dobisë që pasjell për zbatimin e ligjit, suksesi i këtyre operacioneve.

Krimi i organizuar, për nga natyra e qëllimi kriminal që synon të arrijë, ka aftësinë e përshtatjes së menjëhershme të sistemeve të reja të teknologjisë

së informacionit, ndërsa organet ligjzbatuese për arsye logjistike përthithin këto sisteme në një kohë më të vonshme, çka krijon një pengesë serioze në luftën për parandalimin e krimit. Mendojmë që kjo pengesë mund të tejkalohet nëpërmjet krijimit të mekanizmave parandalues në internet me qëllim krijimin e bazave të policimit të internetit dhe bashkëpunimit me përdoruesit e tij. Kjo qasje pro-aktive do të aftësonte organet ligj zbatuese në njohjen e realitetit virtual, njohjen e trendeve, mbledhjen e informacionit digjital dhe reagimin e shpejtë.

Bibliografia

Angelini, D., & Gibson, S. (2007). Organized Crime and Technology. *Journal of Security Education, 2*(4), 65-73. doi:10.1300/J460v02n04_07

Boffey, D. (2021, April 11). *Colombia's cartels target Europe with cocaine, corruption and torture: Armed Belgian police raids have lifted the lid on a sinister new fron in the drug war*. Retrieved May 28, 2022, from Theguardian.com: https://www.theguardian.com/world/2021/apr/11/colombias-cartels-target-europe-with-cocaine-corruption-and-torture

Chini, M. (2021, March 9). *17 tonnes of cocaine and €1.2 million seized in major police operation in Belgium*. Retrieved June 05, 2022, from Brsselstimes.com: https://www.brusselstimes.com/159092/17-tonnes-of-cocaine-and-e1-2-million-seized-in-major-drug-bust-in-belgium-sky-ecc-encrypted-software-organised-crime-the-netherlands

Coe, P. (2015). The social media paradox: an intersection with freedom of expression and the criminal law. *Information & Communications Technology Law, 24*(1), 16-40. doi:10.1080/13600834.2015.1004242

Collier, B. (2020). The power to structure: exploring social worlds of privacy, technology and power in the Tor Project. *Information, Communication & Society, 24*(12), 1728-1744.

Cox, J. (2020, July 2). *How Police Secretly Took Over a Global Phone Network for Organized Crime*. Gjetur June 17, 2022, nga vice.com: https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked

Criminal Intelligence Service Canada (CISC). (2017). *Strategic Early Warning for Criminal Intelligence: Theoretical Framework nad Sentinel Methodology.* Ottawa: Central Bureau. Gjetur April 18, 2022, nga https://publications.gc.ca/collections/collection_2013/sp-ps/PS64-107-2007-eng.pdf

Dijck, J. V. (2013). *The Culture of Connectivity a Critical History of Social Media.* Oxford: Oxford University Press.

Etges, R., & Sutcliffe, E. (2010). An overview of Transnational Organized Cyber Crime. *Journal of Digital Forensic Practice, 3*(2-4), 106-114. doi:10 .1080/15567281.2010.536731

Everton, S. F. (2013). *Disrupting dark networks.* Cambridge: Cambridge University Press.

Gastelum-Felix, S. (2014, September 11). *Social Networks: The Showcase of Organised Crime*. Retrieved May 24, 2022, from Global Initiative.net: https://globalinitiative.net/analysis/social-networks/

Gerdes, L. (2015). *Illuminating dark networks. The study of clandestine groups and organizations.* Cambridge: Cambridge University Press.

Hadjimatheou, K. (2017, November 14). *Policing the Dark Web: Ethical and Legal Issues.* Retrieved June 15, 2022, from European Commission: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c2573eef&appId=PPGMS#:~:text=The%20Dark%20Web%20hosts%20a,of%20child%20sexual%20abuse%20material.

Mercado, R. (2021, July 10). *What is "Vanish Mode" on Facebook Messenger?* Retrieved April 9, 2022, from makeuseof.com: https://www.makeuseof.com/what-is-vanish-mode-on-facebook-messenger/

Morselli, C. (2009). *Inside criminal networks.* New York: Springer.

Morselli, C., & Décary-Hétu, D. (2013). Crime facilitation purposes of social networking sites: A review and analysis of the 'cyberbanging' phenomenon. *Small Wars & Insurgencies, 24*(1), 152-170. doi:10.1080/09592318.2013.740232

Omad, S., Barlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801-823. doi:10.1080/02684527.2012.716965

Pastor, R., & Larsen, H. (2017). Scanning of open data for detection of emerging organized crime threats - the ePOOLICE project. In H. Larsen , J. Blanco, R. Pastor, & R. Yager, *Using open data to detect organized crime threats* (pp. 47-71). Berlin: Springer.

Quirk, R., & Campbell, M. (2015). On standby? A comparison of online and offline witnesses to bullying and their bystander behaviour. *Educational*

Psychology, 35(4), 430-448. doi:10.1080/01443410.2014.893556

Raab, J., & Milward, H. B. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory, 13*(4), 413-439.

Shillito, M. R. (2019). Untangling the 'Dark Web': an emerging technological challenge for the criminal law. *Information & Communications Technology Law, 28*(2), 186-207. doi:10.1080/13600834.2019.1623449

Soudijn, M. R., Vermeulen, I. J., & van der Lesst, W. P. (2022). When encryption fails: a glimpse behind the curtain of synthetic drug trafficking networks. *Global Crime*. doi:10.1080/17440572.2022.2086125

Spadafora, A. (2021, March 20). *Sky Global apparently shuts down following police arrests*. Retrieved June 02, 2022, from Techradar.pro: https://www.techradar.com/news/sky-global-apparently-shuts-down-following-police-arrests

TECHNOLOGY, CYBERCRIME AND THE CRIMINAL LAWYER TRINITY CHALLENGES IN ALBANIA

DR. JONAD BARA[1]

Professor at University of Tirana, Law Faculty, Criminal Department

jonad.bara@fdut.gov.al

ORCID ID: https://orcid.org/0000-0003-4470-9882

DR. BRUNILDA BARA[2]

Law clerk, Legal Services Unit, Constitutional Court of Albania

bruna.bara@gjk.gov.al

ORCID ID: https://orcid.org/0000-0001-7691-5934

At the beginning of the 1970's the world never thought the day would come when technology would become such an important tool for everyday life. 50 years later, people and technology have become inseparable. We use technology in our everyday work, to write a letter, send an email, make a telephone call or video chat, to shop, play games, edit photos and videos, etc. People also use it for 3D architecture and engineering, 3D printing, transactions, the dark web, as well as so many other things. At the same time the use of technology brings about so many challenges, unwanted calls, unwanted emails, bulling, threatening, stealing (identity, money), altering of data, images, information, etc., forging, hacking, digital piracy, use of the dark web for terrorism, mass destruction, as well as so many other activities that the lawmakers decided to call them cybercrimes. The

borderless nature of such crimes makes the use of laws and regulations even more challenging. But what does cybercrime really entails? How prepared are we in a world where technology is changing by the second? How prepared is Albania to fight cybercrime? Do we have the resources, the tools, the means as well as the knowledge and understanding to prosecute such crimes? When it comes to lawyers, how prepared are they to build their defense against such prosecutions? What challenges do they face? This paper aims give a general overview of cybercrime and the challenges faced by the prosecution and the lawyers in such a vast and difficult area, with a special view on the challenges in Albania.

Keyword: *technology, crime, challenges, prosecution, lawyer*

Introduction

On 3 April 1973, Motorola was the first company to mass produce the first handheld mobile phone, while the first successful personal computer went on sale on December 19, 1974. The first mobile operator was introduced in Albania on May 1996,[1] while we only started to have an understanding of what a computer is and what it does only in the early 2000's. Still, the majority of the Albanians learned how to use a computer even later than that. Today we cannot understand our lives without our smart phones, computers, and internet. We are so hooked on finding new ways to explore the new technologies available to us without realizing that perhaps some actions might be not just ethically wrong, but also legal wrongdoings. How far are we wishing to go to protect such freedom and are we wishing to protect just our freedom or that of others too?

The first cybercrimes started with viruses. Everyone has experienced the Trojan horses on their pc's and the corrupted files, loss and leak of data, slow computers (Melissa Viruses, Explore.zip worms) in the beginning of 2000's. In May 2000 computer programming students from the Philippines spread the infamous "I Love You" computer virus that ripped through computers worldwide, causing damages of up to $10 billon. Then came the social networks with MSN Messenger, Yahoo Messenger and then Facebook, and their use not only on PC's but smartphones too. In fact, Google was the first one to introduce the idea of an e-license for its users, similar to a driving license and anyone who watched the Hollywood movie

1 Ramadan Çipuri, *Historia e medias dhe mediatizimi i historisë*, Studime Albanologjike, (2012), 283

The Net with Sandra Bullock can have a slight understanding of the idea of losing your identity. Indeed, the very openness of the internet is both its best asset and its worst liability. Hence, today's technology has brought about so many ways of communication and exchange of personal data which come with a price - the price of our freedom, our money, our image, our rights, leading also to the loss of life.

It has been said since early on that just as prior technological advances – such as the automobile, the telegraph, and the telephone, which brought dramatic improvements for society, also creating new opportunities for wrongdoing, - the same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors, such as education, research, commerce, entertainment, and discourse on public affairs, etc.. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.[2]

Undoubtedly, access to information and communication is a key aspect for participation in society and, in today's society it becomes even more important. We as a country are leaning more and more towards the use of internet with regard to governmental interactions, also aiming at an effective e-justice system. We are now part of the digitalization of our personal data, e-certificates, e-commerce, e-tourism and many other activities conducted online. We're even working towards an e-voting system. While the notion of public service value of the Internet is rather new, it plays an important role as it allows for greater accessibility to public services. Nonetheless, such benefits come with added risks such as loss of personal data and sometimes major data leaks, as was the case of Albania during the last parliamentary elections or end of 2021, which saw personal data of the majority of Albanian citizens, including their income, leaked to the general public.

The Internet presents new investigative challenges for law enforcement agencies at all levels. These challenges include: the need for real-time tracking of all communications not only within the country, but also between

2 The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet, A Report of the President Clinton's Working Group on Unlawful Conduct on the Internet, U.S. Dept. of Justice (2000)

different countries / states; the need to detect sophisticated Internet users who commit illegal acts on the Internet, concealing their true identities; the need for coordination of different legal agencies; the need for a staff trained and equipped with the appropriate technology to detect, investigate, apprehend and prosecute these criminals.

Nowadays law enforcement face the need to assess and determine the source, generally in a very short time, of anonymous emails containing threats (e.g. for bombing a building). The same concerns are raised by other issues such as if a hacker uses the internet to communicate with other computers in 6 different countries, for the purpose of entering a customer's online data, obtaining his credit card data, etc. Through these illegal actions, if law enforcement fails to cooperate and coordinate their activity with their counterparts in other countries to catch the perpetrator, the trust in what is called e-justice will be damaged.

Cybercrime and cyber security. Prosecution and defense challenges

While at the beginning cybercrime was specifically connected and understood to be an unlawful act committed by use of a "computer", nowadays the definition has changed to the use of any "computer technology". Today's smart phones are way smarter that the first computers and can be as powerful, sometimes even more powerful, in the commission of cybercrimes.

The European Commission describes cybercrime as criminal acts committed online by using electronic communications networks and information systems and classifies it in three broad definitions: crimes specific to the internet,[3] online fraud and forgery,[4] illegal online content. [5]

The European Convention on Cybercrime (ETS No. 185) of 2001, also known as the Budapest Convention, provides the substantive criminal cybercrime law: illegal access to the whole or any part of a computer system without right; illegal interception; data interference; system interference; misuse of devices (p.ex. using a computer to illegally access another computer), computer-related forgery, computer-related fraud, child

3 Such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)

4 Such as identity theft, phishing, spamming and malicious coding

5 <https://ec.europa.eu/home-affairs/cybercrime_en>, accessed 06.06.2022

pornography, copyright law infringements (gathering and/or distribution of copyrighted material), etc.

Meanwhile the U.S. Department of Justice broadly defines computer crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."[6]

Cybercrimes can be divided in three major categories: against persons, property, and the state. The lesser but not less important form of cybercrime against a person is cyberbullying, also known also as cyberharassment or internet trolling. Some countries have gone as far as criminalizing such behavior, as is the case of France whose Parliament just recently adopted a new law making school bulling a criminal offence, whereby students or staff can be prosecuted for and those found guilty face a fine of up to 45.000 Euros.[7] Other main forms of cybercrime against the person involve identity theft, and online libel or slander credit card fraud, child pornography and human trafficking.

The second category of cybercrimes is the one against any form of property. Such crimes include acts such as distribution of viruses to destroy other computer technologies, competitor's internet based property, such as p.ex. website crashing, use of computer programs to steal money, illegal access to or distribution of property of any form, including intellectual property, usually protected by a specific set of laws called copyright laws, etc.

The last main category of cybercrimes is the one against the state and its institutions, which mainly includes money laundering, terrorism, and other forms of internet based illegal activities aimed at the justice system and national security. Cybercrime represents a threat to democracy, human rights, the rule of law, and, last but not least, security. Potential threats include cyber-terrorism, that is the shutting down of entire essential infrastructures or the use of computers as weapons – disabling critical systems or threatening whole populations as was the case of Estonia which in 2007 fell under a cyber-attack lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia. Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic. The Council

6 Chris Kim; Barrie Newberger; Brian Shack, *American Criminal Law Review,* (2012), Volume: 49 Issue: 2, p. 443-488

7 <https://www.vie-publique.fr/loi/282708-loi-balanant-2-mars-2022-combattre-le-harcelement-scolaire>accessed 06.06.2022

of Europe prepared a report (Doc. 11325 of 26 June 2007) on the matter discussing important issues at stake for all countries such as how to prevent cybercrime against state institutions in member and observer states.

In this regard, at the end of 2020, following the landmark Court of Justice ruling in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* ("Schrems II") of July 16-th, we all started to receive notifications via email on the use of our personal data by third parties and more extended information on those parties. Today we open an internet page and a pop up screen asks whether we want accept cookies or whether we want to share our information with third parties. All this comes as a result of the continuous efforts of EU countries to protect personal and private data. On 25 March 2022, the European Union and the US announced that they have reached an agreement in principle on a new framework for transatlantic data flows. This follows many months of legal uncertainty following the ruling which declared the previous EU-US Privacy Shield invalid.

When it comes to cybercrimes, another issue is money laundering and the complications it brings to state economy and finances which is often closely linked to terrorism. While some hackers are fraudsters who are attempting to steal identities or other valuable information for financial gain. Other hackers are state actors who are seeking to gain intelligence on, or to harm, their adversaries. Others are politically motivated individuals or organizations seeking to make a point.

Another tool at the hands of European prosecutors in their fight against such crimes is the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 2005 (CETS 198). However the fight against cybercrime is not as easy as it seems. While some cases might be easier and more clear on who the perpetrator is, others require special skills in the area of cyberspace which the common prosecutor does not have. Gathering of evidence in cybercrime cases and the investigation thereof, and in particular hacking, is of complex nature and requires particular skills. Hence the prosecuting authorities need to collaborate with cybercrime units in order to establish the truth and find out the perpetrator. While a state can have the necessary resources to establish the offence and/or the offender, the task becomes even more difficult for the defense lawyer, who the majority of times does not have the necessary financial means to find experts in the field of cyber to challenge the prosecution. Furthermore, cybercrime evidence can be difficult to understand for the lawyer and without understanding the case in

its merits, establishment of the facts, the way evidence was gathered and/or handled by the prosecution can be difficult to challenge. Even more so, such cases can be difficult for judges too, which makes rendering justice even more difficult.

European Court of Human Rights' case-law on the use internet

Majority of cases decided upon by the European Court of Human Rights (ECtHR) with regard to use of internet mainly deal with matters of use of personal data by the government of private entities and the way such data is stored and protected, which mainly fall within the protection of Article 8 of the European Convention on Human Rights (ECHR), right to private and family life. Some cases deal with the right to property, mainly intellectual property of freedom of speech on the internet.

In *Premininy v. Russia*,[8] the case concerned two Russian nationals living in Russia. They were detained in Russia on suspicion of hacking into the online security system of an American bank, "Green Point Bank", in 2001 and stealing its database of clients and extorting money in exchange for the promise not to publish that database on the Internet. The cases were brought before the ECtHR on violation of Articles 3 and 5 of the ECHR.

In *Perrin v. the United Kingdom*,[9] the case concerned the applicant's conviction and sentence for publishing an obscene article on a website. The applicant was a French national living in the United Kingdom. The website was operated and controlled by a company based in the United States of America that complied with all the local laws and of which the applicant was a majority shareholder. The ECtHR declared the application manifestly ill-founded within the meaning of Article 35 § 3 of the Convention and held that as a resident in the UK, the applicant could not argue that the laws of the United Kingdom were not reasonably accessible to him. Moreover, he was carrying on a professional activity with his website and could therefore be reasonably expected to have proceeded with a high degree of caution when pursuing his occupation and to take legal advice.

With regard to Article 8 of the ECHR, ECtHR has discussed the issue of protection of personal information in many cases. In *Flinkkilä and Others*

8 Application no. 44973/04, 10 February 2011

9 Application no. 5446/03, ECHR 2005-XI

v. Finland,[10] the applicants - 4 journalists, were convicted for invasion into of the private life of the state official's female friend, complained that their freedom of expression had been violated as they were punished for reporting on a high profile criminal case involving a state official. The ECtHR held that the freedom of expression has to be balanced against the protection of private life guaranteed by Article 8 of the Convention. The concept of private life covers personal information which individuals can legitimately expect should not be published without their consent and includes elements relating to a person's right to their image.

In *Alkaya v. Turkey*,[11] the ECtHR eld that the disclosure of the home address of a Turkish actress (pictured) in a newspaper article was a violation of her right to private life under Article 8 ECHR. In *Von Hannover v. Germany (no. 2)* [GC],[12] ECtHR has also held that photographs or videos which contain a person's image will fall within the scope of Article 8. In fact the right to the protection of one's image presupposes the individual's right to control the use of that image, including the right to refuse publication thereof. In *Peck v. the United Kingdom*,[13] ECtHR held that the publication of material obtained in public places in a manner or degree beyond that normally foreseeable may also bring recorded data or material within the scope of Article 8 § 1.

Many cases before the ECtHR concern data protection by the state. The compiling, storing, using and disclosing of personal information by the State, for example in respect of a police register, amounts to an interference with one's right to respect for private life as guaranteed by Article 8 § 1 of the Convention.[14]

In *B.B. v. France*[15] and *Gardel v. France*[16], the issue was whether inclusion on a national database of those who had committed sexual offences amounted to a violation of Article 8. This was in the context of the data being retained for 20-30 years depending on the seriousness of the offence committed. Finally, the Court came to the view that there was no violation of Article 8 in either case, given that a procedure existed for

10 Application no. 25576/04, 6 April 2010

11 Application no. 42811/06, 9 October 2012

12 Applications nos. 40660/08 and 60641/08, 07.02.2012

13 Application no. 44647/98, 28.01.2003

14 *Leander v. Sweden,* Application no. 9248/81, 26.03.1987, § 48

15 Application no. 5335/06, 17.12.2009

16 Application no. 16428/05, 17.12.2009

requesting the data to be removed from the database. The Court took into consideration the very serious nature of the offences committed and the public interest in the maintaining of such databases.

In *Dalea v. France*,[17] the applicant complained that retention of data on him in the Schengen information system had the effect that he was not allowed to travel for personal or professional reasons within the Schengen area (he was refused the relevant visas). His application was declared inadmissible; under Article 8 the Court reasoned *inter alia* that he had had the opportunity of challenging the proportionality of this measure before various domestic bodies.

In *K.U. v. Finland*,[18] the case concerned posting of an offensive advertisement on an internet dating site in the name of a 12-year-old Finnish national, K.U, by an unknown person. The advertisement stated that the applicant was looking for an intimate relationship with a boy of his age or older. A criminal investigation was instituted, which failed to identify the perpetrator, who posted the advertisement. This was due to the fact that the Internet Service Provider of the dating site refused to divulge the details, considering itself bound by the confidentiality of telecommunications as defined under the Finnish law. The Court reviewed several international instruments on the subject of information technologies and criminal procedure law connected with information technologies. It noted that the Government and the legislator are required to follow societal and technical developments and amend domestic legislation to align them with international obligations.

Internet is also closely linked to freedom of expression and many cases before the ECtHR involved limitations to such freedom. One case worth mentioning is *Mouvement raëlien suisse v. Switzerland*[19]. The case concerned a non-profit association with the stated aim of making initial contact and developing good relations with extraterrestrials. In 2001 it sought permission from the police to put up posters which featured pictures of extraterrestrials' faces and a flying saucer and displayed the Movement's Internet address and telephone number. Permission to put up the posters was refused, and subsequent appeals by the association were all dismissed. For the ECtHR it was undisputed that the poster in itself did not contain anything unlawful or shocking to the public, either in its wording

17 Application no. 964/07, 02.10.2010

18 Application no. 2872/02, 02.12.2008

19 Application 16354/06, 13.01.2011

or in the illustrations. However, it featured, in bold type, the association's website address, which linked to the Clonaid site, where specific cloning services prohibited by law were on offer to the public. Since the websites in question were per se accessible to everyone, including children, the public impact of the posters would have been amplified and the State's interest in prohibiting the poster campaign was all the greater.

Challenges of cybercrime in Albania

In last years the majority of Albanian citizens were subjected to loss of huge amount of personal data. The first on was during the recent general elections of 2021 when personal data, such as name, last name, ID number, were leaked to the public, as well as information on individuals' voting preferences. The second one was in December last year when another major leak of personal data occurred, consisting on ID number, salary, job description, and in some cases home address too. Such information included not only public employees, but the private sector too. First major concern was obviously the data leak itself, second the fact that apart the job description, the home address was sometimes included in the information, putting people's safety at risk.[20]

As for many other foreign countries, at the beginning of 1995 when the Albanian Criminal Code of the democratic state was enacted by law no. 7895 of 27.01.1995, the legislator did not have any understanding of cyber acts. The code provided for general criminal offences such as violation of secrecy of correspondence (Articles 123 and 255), theft (Article 134), bank robbery (Article 136), copyright (Articles 148 and 149), destruction of property (Article 150), forgery of money, bonds, documents or stamps (articles 183 and continuous), destruction of state defense systems (Article 215).

The major changes in this regard came at the end of 2088, with the enactment of law no. 10023 of 27.11.2008 "On several additions and changes to law no. 7895 of 27.01.1995 "The Criminal Code of the Republic of Albania", which introduced the notions of cybercrime, such as criminal offences in the area of information technology (Article 1), distribution by computers of materials pro genocide or crimes against humanity (article

20 Distribution of public employees' personal data is at present being considered by the European Court of Human Rights in the case *Gashi and Gina v. Albania*, communicated case no. 29943/18, on account of the fact that the assets declaration of the applicants had been disclosed to the media.

11), racist or xenophobic threats through computer systems (Article 12), distribution of racist or xenophobic materials through use of computer systems, public insults of racist or xenophobic nature through use of computer systems (Article 13), computer fraud (Article 15), interference in computer systems (Article 23) and unauthorized access to a computer system (Article 53).

Today, as part of its efforts to become an EU member, Albania has intensified the harmonization of its legislation with *acquis communautaire*. However, the harmonization of the legislation should go hand in hand with the building of the necessary infrastructure and human resources to combat cybercrime. In this regard, a special attention should be paid to the capacity building, training and exchange of good practices with international counterparts which should include participants from both prosecution and state police IT services, judicial police officers, prosecutors, as well as participants from other law enforcement agencies. Similar trainings should also be part of the Albanian Advocacy Chamber, in order that lawyers get to have a general understanding of what cybercrime entails, what procedural guarantees a cybercrime defendant has *vis à vis* the prosecution, how prosecution's findings can be challenged and what steps can be taken to guarantee equality of arms. Furthermore, another important measure is the policy building and public awareness on cybercrime, paying particular attention to the young generation who, in a technology developing by the hour, can be just as skilled when committing such crimes as the adults.

Conclusions

The best way to combat cybercrime is prevention. With the explosive growth of the Internet worldwide, computer crimes increasingly are prone to have international dimensions. The main challenges facing the prosecution are quick information sharing, interstate agency collaboration as well as interstate collaboration between counterparts, harmonization of countries' criminal laws, locating and identifying perpetrators across borders, securing electronic evidence of their crimes so that they may be brought to justice. Complex jurisdictional issues arise at each step.

To be effective, any overall strategy must include the owners and operators of the nation's computer networks. They are the first line of defense and have the responsibility to take reasonable measures to ensure that their systems are secure. They are also in the best position to detect

intrusions and take the first critical steps to respond.[21]

While Albania is on the right path to the harmonization of its legislation with the legislation of the European Union, there is still much to be done on the fight against cybercrime. Main focus points should also be capacity building, information sharing, exchange of experiences, as well as raising general public awareness.

Bibliography

Books

Çipuri R., *Historia e medias dhe mediatizimi i historisë*, Studime Albanologjike, (2012)

Journals

Kim Ch., Newberger B., Shack B., *American Criminal Law Review,* (2012), Vol.: 49 (2)

Reports

The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet, A Report of the President Clinton's Working Group on Unlawful Conduct on the Internet, U.S. Dept. of Justice (2000)

Richard P. Salgado, Working with Victims of Computer Network Hacks, USA Bulletin (March 2001)

How to prevent cybercrime against state institutions in member and observer states? Council of Europe Doc. 11325 (2007)

Conventions

The European Convention on Cybercrime (ETS No. 185)

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 2005 (CETS 198)

The European Convention on Human Rights (ECHR)

European Court of Human Rights' case law

Alkaya v. Turkey, Application no. 42811/06

21 Richard P. Salgado, Working with Victims of Computer Network Hacks, USA Bulletin (March 2001)

B.B. v. France, Application no. 5335/06

Dalea v. France, Application no. 964/07

Flinkkilä and Others v. Finland, Application no. 25576/04

Gardel v. France, Application no. 16428/05

Gashi and Gina v. Albania, communicated case no. 29943/18

K.U. v. Finland, Application no. 2872/02

Leander v. Sweden, Application no. 9248/81

Mouvement raëlien suisse v. Switzerland, Application 16354/06

Peck v. the United Kingdom, Application no. 44647/98

Perrin v. the United Kingdom, Application no. 5446/03

Premininy v. Russia, Application no. 44973/04

Von Hannover v. Germany (no. 2) [GC], Applications nos. 40660/08 and 60641/08

EU Court of Justice case law

C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* ("Schrems II")

Websites

https://ec.europa.eu/home-affairs/cybercrime_en

https://www.vie-publique.fr/loi/282708-loi-balanant-2-mars-2022-combattre-le-harcelement-scolaire

"ROLI I TEKNOLOGJISË NË PARANDALIMIN DHE LUFTIMIN E KRIMIT TË ORGANIZUAR, KRIMIT FINANCIAR DHE KORRUPSIONIT".

"TEKNOLOGJIA DHE NDIKIMI I SAJ NË KRIMIN E ORGANIZUAR"

MSC. ARFJONA DUKA

DR. IV ROKAJ

Krimi i organizuar është një nga fenomente më të përhapura në mbar botën, veçanërisht në dekadat e fundit ky fenomen është përhapur ndjeshëm ndër të tjera edhe në vendet e rajonit të Ballkanit Perëndimor.

Përhapje kjo e cila i ka dhënë krimit të organizuar dhe ndikimit të teknologjisë së zhvilluar, në ralizimin e veprave kriminale vlera aktuale. Të dy këto fenomene për shkak të karakterit dinamik të tyre paraqesin interes të vazhdueshëm për, trajtimin dhe studimin e tyre, ndaj dhe punimi ynëështë përqëndruar në trajtimin e krimit të organizuar dhe përdorimi i teknologjisë.

Shoqëria është vazhdimish në zhvillim. Natyra e këtij përparimi social është në rritje progresive me atë të evoluimit të teknologjisë. Shoqëria duke synuar krijimin dhe përfitimin e fasiliteteve në mënyrën e dhënies dhe marrjes së shërbimeve, komunikimeve apo çdo lehtësire tjetër, në mënyrë të natyrshme është bërë kërkuese dhe indikator nxitës për krijimin e teknikave teknologjike, dhe realizimin e një bote të hapur. Kjo kërkesë apo nxitje për përdorimin e metodave teknologjike ka ardhur në mënyrë të përshpejtuar dhe entuziaste pa vlerësuar ndikimin e teknologjisë në jetën, lirinë dhe privatësin dhe të drejtat me karakter individual dhe atë sociale. Në epokën

që jetojmë teknologjia është e pranishme në çdo aspekt të jetës, gjë e cila e ka bërë shoqërinë të jetëeekspozuar ndaj çdo ndërhyrje apo sjellje kriminale në jetën personale dhe sociale.

Teknologjia mund të përkufizohet si një grup njohurish shkencore të materializuara në mekanizma të sofistikuar që synojnë të kënaqin nevojat njerëzore të lidhura me progresin ekonomik dhe shoqëror. Teknologjia vërtet priret të përmirësojnë aspektet e jetës së përditshme,[1]por përdorimi i pakufizuar dhe i pakontrolluar përbën një faktor riskutë pa evitueshëm për çdo individ.

Në shumë vende të zhvilluara teknologjia ka ndikuar në zhvillimet ekonomiko-sociale të cilat përbëjnë edhe faktorët dominant në rritjen e kriminalitetit. Në këtë mënyrë teknologjia jo vetëm ka ndikuar por edhe ka ndihmuar në rritjen e kriminalitetit.

Krimi si fenomen ka ekzistuar që në shoqërit e hershme por ajo që evidentohet në shoqërit modern është pikërisht forma e ndryshme në të cilat shfaqet krimi. Format e reja të shfaqjes se krimit kanë tendenc të tejkalojnë format tradicionale duke sjell forma të avancuara dhe teknologjike.

Veç formave të zakonshme të krimit sot është evidentuar ndjeshëm tendenca e kryerjes së krimit në forma të organizuara.Koncepti i krimittë organizuarështë sanksionuar për herë të parënë vitin 1896 kur është përdorur në raportin vjetor të shoqatës për parandalimin e krimit, në New York.[2]

Ky fenomen ka ardhur duke u zhvilluar dhe është përhapur ndjeshëm gjatë dekadave të fundit të shekullit të XXI, duke revolucionalizuar format e kualifikuara të shfaqes së kriminalitetit.

Mënyra e shfaqes së krimit të organizuar

Krimi i organizuarpërbën një fenomen kompleks që konsiston në kryerjen e veprimeve të kundraligjshme dhe me rrezikshmëri të lartë shoqërore. Rrezikshmëri e cila shfaqet në dy dimensione; si nëformën e kryerjes së krimit të organizuar, për nga natyra e subjekteve të angazhuara ashtu edhe

1 John Stephens, 23 avantazhe dhe disavantazhe të teknologjisë, botuar më 25.janar 2021 https://sq.warbletoncouncil.org/ventajas-desventajas-tecnologia-2854 (dt. 01.10.2022).

2 Organized Crime in Europe", *Concepts, Patterns and Control Policies in European Union and Beyond, red*. Cyrille Fijnuat and Letizia Paoli, "Springer", Holandë 2004 fq.23.
Hysi.V, "*Kriminalogjia*", Tiranë 2010, fq.274.

përnga metodologjia apo mekanizmi i përdorur në realizimin e qëllimit kriminal.

Të gjithë këto faktor rrezikshmërie përforcohen ose shtohen kur realizimi i krimit dhe veçanërisht ai i krimit organizuar mbështetet ose realizohet nëpërmjet përdorimit të teknologjisë së avancuar e cila përbën një risi dhe në të njëjtën kohë edhe kërcënim për qëndrueshmërinë, besueshmërinë dhe stabilitetin.

Lidhur me subjektete e krimit

Krimi i organizuar në lidhje me subjektet e kryerjes së krimit, nënkupton një grup individësh të strukturuar për nga mënyra funksionale, në një bashkim të disiplinuar me qëllim të përbashkët kriminal,[3] duke krijuar në këtë mënyrë një frymë të qëndrueshme bashkëpunim, brenda grupit të organizuar. Referuar formës së bashkëpunimit dhe organizimit brenda grupit Kodi Penal Shqiptar në nenin 28 ka sanksionuar forma të veçanta tëbashkëpunimi duke përfshirë organizatat kriminale, organizata terroriste,bandat e armatosuradhe grupin e strukturuar kriminal, të cila përbëjnë edhe mënyrën e dukshme të shfaqesëpublike të krimit të organizuar.

Krimi i organizuar në lidhje me subjektet paraqet rrezikshmëri të dyfishtë, si në lidhje me numrin e antarëve brenda grupit ashtu edhe në lidhje me rrezikshmërinë individuale tëçdo antari.[4] Antarët më mënyrë të vullnetshme dhe të organizuar japin kontributin e tyre jo vetëm në kryerjen e veprave penale me qëllim të përbashkët kriminal, por edhe në ofrimin e aksesit në rrugën e përdorimit të teknologjive të sofistikuara, duke forcuar veprimtarin dhe penetrimin e krimit të organizuar edhe në strukturat institucionale që deri dje konsideroheshin të padepërtueshme.

Zhvillimi i teknologjisë i inkorporuar në evoluimin e shkencës kabërë të mundur identifikimin e sjelljes kriminale që në moshë të herëshme.[5] Sjellje këto të cilat stimulohen nëpërmjet moduleve të shkurtra informative, nëpërmjet krijimit të një mjedisi konfort për individët në pamundësi për tu përshtatur me kërkesat social-shoqërore. Kjo dobësi e zinxhirit social dhe rritjae ndikimit teknologjik ka tendencë të përdoret nga krimi i organizuar, i cili në këtë mënyrë rekruton antarë të rinjë, zgjeron strukturën e grupit

3 Adamoli,S; Di Nikola, A; Savona. E etj.”*Organized Crime around tha world*”, Helsinki, 1998. Fq.4

4 Harring. J, “*E drejta Penale*” vol.1 , Tiranë, tetor 2013, fq .10.

5 Dragoti.E ,”*Psikologjia ligjore e krimit*”, Tiranë, fq. 23

dhe thellon depërtimin e tij, nëpërmjet përdorimit tëburimeve njerëzore edhe teknologjisë së avancuar.

Përdorimi i teknologjisë përbën një revolucion global. Referuar statistikave, sot teknologjia përdoret mbi 93% nga grup moshat 16-35 vjeç, mbi 83% nga grup moshat 35-45 dhe mbi 73 % nga moshat 45-65 veç. Përdorimi i tekonologjisëështë shtrirë në mënyrë të pakufizuar në jetën individuale dhe sociale te çdo person[6], e cila shpesh shërben si promovues i sjelljeve që vinë në kundërshtim me ligjin.

Përhapja e shpejtë dhe në rritje e përdorimit të teknologjisë, është shëndërruar në mbështetësen krysore tëaktivitetit kriminal.

Evoluimi dhe aksesi i risive teknologjike shërben sot si njëmjet për komunikimin dhe ndërveprimin e antarëve të grupit. Teknologjiaështë bërë një mjet efikas në garantimin e vazhdimësisë dhe qëndrueshmërisë së grupit. Zhvillimi i teknologjisë ka eleminuar barrierat fizike të komunikimit duke krijuar në këtë mënyrë fasilitete të cilat përveç përdorimit në jetën sociale janë integruar në mënyrë të vrullshme edhe në kryerjen e veprave penale.[7] Teknologjia ka bërë të mundur bashkimin dhe bashkëpunimin e antarëve të grupit të organizuar kriminal, pavarësishtë largësisë gjeografike, vendndodhjes dhe rrethanave të tjera. Teknologjia konsiderohet sot një mënyrë efikase e kryerjes së shërbimeve në distancë duke ofruar në këtë mënyrë modele të reja të shfaqes së kriminalitetit.

Zhvillimet teknologjike kanë sofistikuar mënyrë e kryerjes së krimit të organizuar duke bërë të mundur qëardhja e pasojave kriminale të realizohet si nga:

1- Veprimet e drejtëpërdrejta, ose veprimiet mekanike të vetekzekutorit në cilësin e subjekteve të angazhuara në krimi, i cili për realizimin e qëllimit dhe ardhjesë së pasojës kriminale priret të përdor mjete dhe metoda të sofistikuara të cilat pengojnë zbulimin e gjurmeve dhe vështirësojnë identifikimin e autorit.

2- Gjithashtu përdorimi iteknologjisë në krimin e organizuar ka ofruat mundësi tekniketë cilat bëjnë të mundurqëvullnetikriminal brenda grupit të organizuar të manifestohet në pasoja konkrete jo më nga veprimet fizike të antarëve të grupit, por nëpërmjet përdorimit të inteligncës artificiale e cila përbën një nga risit revolucionare të

6 http://pxweb.instat.gov.al:8080/index.php/789122/lang-sq (INSTAT 2022)

7 https://teknologjia2.weebly.com/(dt.29.10.2022).

teknologjisë.[8]

Struktura e organizuar e krimit veç hierarkisë strukturore në ndarjen e funksioneve manifestohet edhe në një formë tjetër, e cila lidhet ngushtë me angazhimin e grupit kriminal nëpërmjet kryerjes së veprimeve ose mosveprimeve të kundraligjshme[9]për të identifikuar metodat inovator, mjete teknike dhe përdorur paisje teknologjike në realizimin e qëllimit kriminal. Në këtë aspekt forma e organizuar e krimit manifestohet si një tërësi veprimesh të organizuara sipas një plani të paramenduar, në kuadër të një qëllimi tëmire-orientuar kriminal.

Nëmbështetje të realizimit të strategjisë kriminale, strukturat e krimit të organizuar angazhohen në mënyrë të vazhdueshme në krijimin e një infrastrukture materiale të përparuar që ndihmon aktivitetin e tyre.

Krimi i organizuar shfaqet në forma diverse[10]dhe vazhdimisht promovon forma të reja, dhe mëtë avancuara.

Në varësi të formës se krimit të organizuar përcaktohet edhe meksanizmi për realizimin e strategjisë kriminale edhe metodologjia apo mjete e sofistikuara që do të përdoren për realizimin e qëllimit kriminal.

Referuar mjeteve të përdorura në veprimtarin kriminale i ndajmë ato në dy kategori.

1- Mjete - të drejtëpërdrejta- janë ato mjetë të cilat përdoren nëkryerjen e veprimtarisë kriminale të cilat shkaktojnë në mënyrë të drejtëpërdrejtë pasojën kriminale. Vitet e fundit është reflektuar furnizimi i grupeve kriminale me mjete të cilat vënë në rrezik jetën dhe shëndetin ku përmendim eksploziv të telokomanduar, dron vrasës, armë dhe municione të sofistikuara që reflektojnë rrezikshmëri të lartëdhe zbulueshmeri të ulët.

Krimi i organizuar duke integruar në strukturat e tij teknologjin e avancuar po cënon në mënyrë të vazhdueshme edhe të drejta të tjera me karakter kushtetues të cilat janë të fokusuara në ofrimin e lirisë dhe privatësisë dhe mbjojtjen e të dhënave personale për çdo individi. Një nga format më të përhapura të krimit të organizuar është ai kibernitik. Në këtë rast krimi

8 Ajo është një nga llojet e zhvillimit të teknologjisë, e cila bënë të mundur që kompjuteri të ketë aftësi të veprojë si qënje njerëzore. https://sq.wikipedia.org/wiki/Inteligjenca_artificiale(dt.01.10.2022).

9 Muçi. SH. "*E drejta penale Pjesa e Përgjithshme*", Tiranë 2016,fq.115.

10 Referuar nenit 3 të Konventës së Kombeve të Bashkuar, "*Kundër krimit të organizuar ndërkombëtarë*"

i organizuar nëpërmjet përdorimit të sistemit operative kompjuterike, hardware-ve dhe software-ve të avancuara arrin në distancë të marrë informacione të karakterit sekret, personal dhe institucional të cilat krijojnë një hapësirë tërheqëse për zhvillimin e krimit.[11]

Përdorimi në masëi teknologjisë kompjuterike e bënë atë një hapësirë tëcënueshme dhe për rrjedhojë një terren shumë fertil[12]i cili i ofron krimit të organizuarkomoditet për tëidentifikuar dhe sulmuar pikërisht ato shënjestra qëi ofrojnëhapsirë veprimtarisë kriminale.

2- Në këtë vështrim, krimi i organizuar mund tëasistohet në realizimin e veprimtarisë kriminale edhe nga mjete indirektë të cilat nuk e shkaktojnë pasojnë kriminale por ndihmojnë nërealizimin e komunikimit, mbledhjen e informacionit dhe krijimin e kushteve që lehtesojnë kryerjen e krimit.

Lidhur me këtë fenomen përmendim mjetet teknologjike që ofrojnë komunikim të inkriptuar për antaret e grupit kriminal siç është Encrochat, Matrix, Telegram, të cilat janëpaisje telefonike të modifikuara android, që përdorin programe të koduara dhe i rezistojnë përpjekjeve të ligjshme për të fituar akses në përmbajtjen e tyre.[13]Këtopajisjet kanë sisteme operative të dyfishta - një normal dhe një i fshehur për të kryer mesazhe sekrete,e cila garanton anonimitetit maksimal dhe mbron grupet kriminale nga identifikimi i tyre dhe për rrjedhojëofron një sistem efikas që parandalon goditjen e krimit të organizuar duke ofruar në këtë mënyrëhapsirëpër konsolidimin e veprimtarisë kriminale.

Tregtia e lirë dhe globale e bënë lehtësisht të mundur shtënien në dorë të mjeteve tekonologjike. Përmendim në këtë rast IMSI-Catcher apo përgjuesve të ndryshëm të cilët ofrohen sot në forma, përmasa dhe me aplikacione të shumëllojshme që mundësojnë lokalizimin, fotografimin, përgjimin audio dhe viziv të personit.

Krimi i organizuar ka një nivel të caktuar stabiliteti ekonomik të cilën nuk e ngurtëson kur bëhet fjalë për investime teknologjike qëi shërbejnë veprimtarisë kriminale, pasi në këto grupe kjo konsiderohet një investim i kthyeshëm. Ndaj, në veprimtarin kriminale reflektohet përdorimi i larmishëm i mjeteve apo paisjeve qëmundësojnë në mënyrë të pa kufizuar informimin

11 Strategjia për mbrojtjen kibernitike 2018-2020. Fq.3. (https://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf).

12 https://sq.wikipedia.org/wiki/Krimet_kibernetike(dt 30.09.2022)

13 ps://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678 (dt.29.09.2022)

e struktuarave të organizuara kriminale.

Duke vlerësuar zhvillimet e mënyrës së organizimit, metodat e kryerjes së krimit dhe mjetet e përdoruar në realizimin e veprimtarive kriminale ndër vite, padyshim qëteknologjikaka reflektuar në mënyrë konsekuente një ndikim mbështetës ndaj zhvillimit dhe promovimit të krimit të organizuar. Ky qëndrim pasqyrohet edhe nga të dhënat statistikore të viteve të fundit. Konkretish nga vitet 2017 e deri në viti 2021 numuri i veprave penale të evidentuara është rritur afërsisht me 3%, ndërsa numuri i veprave penale të dënuar për të njëjtën periudhëështë ulur me afërsisht 8%.[14]Këto tregues konfirmojnë se krimi i organizuar po operon në mënyrë tepër të sofistikuar, dhe profesionale, gjë e cila vështirëson dënimin e tij.

Karakteri global dhe bashkëpunimi ndërkombëtarë për parandalimin e Krimit të organizuar.

Krimi i organizuar është një dukuri e panjësuar[15] e cila karakterizohet nga forma kriminaliteti që evoluojnë me shpejtësi. Për një kohë të gjatë krimi i organizuar po vepron dukshëm në vendet e Europës Përendimore, Qëndrore dhe Lindore duke kryer aktivitete të larmishëm kriminale si, trafikimi i paligjshëm i lëndëvë narkotike, armëve dhe qenieve njërëzore.

Këto forma kriminaliteti karakterizohen nga mungesa e kufijve nacional. Në këtë aspekt vihet re tendenca e krimit të organizuar për të përfituar nga hapsirat e reja që ofrojnë paqëndrueshmëri politike,[16] ekonomike dhe diversitet social.

Organizimi istrukturave kriminale dhe metodat e përdorura prej tyre evoluojnë me shpejtësi sirezultat i ndryshimeve strukturore në nivel kombëtar dhe ndërkombëtar. Globalizimi ikrimittë organizuar është një fenomen dinamik qëi përshtatet vazhdimisht rrethanave dhe nevojave të kohës.

Kjo strukture e organizuar tenton në mënyrë të vazhdueshme të shtrijë veprimtarin e saj drejtëhapsirave të reja.[17] Falë risive teknologjike, që mundësojnëinformim, e komunikim cilësore dhe të shpejtë, veprimtaria e krimit të organizuar po hamonizohet drejtëndërkombëtarizimit.

---

14 http://instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/krimet-dhe-drejt%C3%ABsia-penale/#tab2

15 Savona.E, "*Measuring organized crimi: An international prespective*", botuar në: "Forum on crime and society" vëllimi 5, nr.1, United Nations, New York, 2009 fq. 21.

16 Udhëzues i strategjisë për krimin e Organizuar, Kombet e Bashkuara Vjena 2021. Fq.1

17 Hysi.V, "*Kriminalogjia*", Tiranë 2010, fq.283

Në kuadër të globalizimit dhe zhvillimeve teknologjike grupet kriminale kanë zgjeruar strukturat e tyre duke rritur shkallën e rekrutimit të njerëzve. Ato kanë përfshirë në veprimtarinë e grupit kriminal antarëme shtetësi të ndryshme dhe diversitet profesional[18]të cilët kanë aftësi të ofrojnë shërbime të larmishme me të cilat ndihmojnë dheorientojnëveprimtarinë kriminaledrejtë rritjes ekonomike dhe forcimittë pushtetit kriminal.

Grupet kriminale veç aktivitetit të pavarur kriminal kanë shfaqur qasje drejtë bashkëpunimit me grupet të tjera kombëtare dhe ndërkombëtare[19]. Grupet e krimit tëorganizuar gjithnjë e mëtepër po thellojnë ndërveprimin e përbashkët në veprimtarinë kriminal nëpërmjet komunikimit, ofrimit tëmallrave, shërbimeve dhe ekspertizë. Kjo formë bashkëpunimi brenda komunitetit kriminal po krijon një zinxhirë furnizimi transnacional në një tregglobal të lidhurteknologjikisht, duke krijuar një rrjet kriminal, të fokusuar në dominimin e hapsirave te reja ndërkombëtare dhe zgjerimin e veprimtarisë.

Krimi i organizuar përbën trendin e koheve modern.Kjo përhapje e krimit të organizuar me dinamik progresive ka fuqizuar frymën e kriminalitetit dhe ka shtuar rrezikshmërin e depertimit të krimit të organizuar në të gjitha strukturat shoqërore,politikedhe qeverisëse.

Krimi i organizuar është njëstrukturuar me natyrë heterogjene dhe tepër fleksibël, që dallohet për organizim të fortë, ndarje të qartë dhe të saktë të roleve, detyrave dhe përgjegjësive ndërmjet antarëve.[20]Krimi i organizuar është një strukturë me influencë, e cila ka demostruar një kombinim tëaftësinë dhe forcës për të depërtuar dhe zgjeruar veprimtarinë kriminale në nivel ndërkombëtar. Zhvillimi dhe përhapja i një strukture të tillë me rrezikshmëri të lartë cënon seriozisht stabilitetin social dhe ligjor.

Krimi dhe në veçanti aii organizuar është një fenomen që kërcënon seriozisht demokracin, shtetin e së drejtës dhe të drejtat e njeriut.[21] Në këtë vështrim strukturat kombëtare duhet të impenjohen në mënyrët të vazhdueshme për të krijuar politika dhe strategji që luftojnë krimin e organizuar, si edhe të ndërmarrin nisma që synojnëazhornimine kuadrit ligjor me risitëinovative tëteknikave kriminale.

---

18 Adamoli.S, Di Nicola.A, Savona. E, etj. "*Organized Crime around the World*", HEUNI, Helsinki 1998 fq10.

19 Hysi.V, "Kriminalogjia", Tiranë 2010, fq.284

20 Po aty

21 Projekti Rajonal CARPO- "*Raporti mbi gjendjen e krimit të organizuar dhe krimit ekonomik në Europën Juglindore*" Strasburg, gusht 2006 fq.5.

Zhvillimii teknologjisë dhe përdorimi i saj nga krimi i organizuar e ka forcuar dukshëm këtë fenomen dhe i ka siguruar asaj një mburoj pazbulueshmërie duke e vendosur në pozita të favorshme dhe gati dominante në raporte me mekanizmat e kësaj natyre që përdorin organet dhe sturkturat kombëtare të ngarkuara me ligj për tëluftuar krimin. Situatë kjo e cila ul ndjeshëm efiçencen dhe efikasitetin në parandalimin dhe zbulimine krimit të organizuar.

Në këtë vështrim nismat ligjore duhet të reflektohen edhe transplantohen edhe në infrastruktura materiale. Krahas trajtimit ligjor strukturat kombëtare duhet tështrijnë vëmendjen e tyre edhe në investime materialo-teknologjike të avancuara, dhe të sigurta të cilat mundësojnë gradualisht ngadalësimin e shtrirjes së krimit të organizuar deri në goditjen përfundimtare të tij.

Angazhimi në nivle kombëtar duhet të jetë në harmoni dhe të synojë rritjen e bashkëpunimit ndërkombëtarë, pasi krimi i organizuar transnacional është një sfidë globale që kërkon zgjidhje globale.[22]Në këto kushte lufta kundër krimit të organizuar kërkon aplikimin e mekanizmave efektivë tëbashkëpunimit në nivel kombëtar dhe ndërkombëtar, ndaj duhet të krijojen lehtësira që promovojnë rritjen e kësaj fryme, pasi kjo është e vetmia mënyrë që arrin të godas krimin e organizuar dhe të dobësoj strukturat e tij.

Bashkëpunimi ndërkombëtarë nëparandalimin dhe luftimin ekrimit të organizuar transnacional promovohet edhe nga neni 1 të Konventës "KundërKrimit të Organizuar" e cila synonë të inkurajojë vendet të marrin masat e duhura nëzhvillimin dhe forcimin e kuadrit të tyre strategjik kundër krimit të organizuar.Realizimi i një partneriteti bashkëpunues në nivel ndërkombetar është thelbësor në arritjen e rezultateve. Bashkëpunimi aktiv dhe zhvillimi i shkëmbimit ndërkombëtar të informacionit[23], siguron rezultate positive në procesin e goditjes së krimit duke lëkundur ndjeshëm strukturat e qëndrushme të tij. Në këtë pikë struktuarat kombëtare dhe ndërkombëtare duhet të rrisin vigjilencën dhe angazhimin e tyre nëpërmjet krijimit dhe zbatimit të strategjive të përbashketa. Këto struktura duhet të jenë të gatshme të ofrojnë ndihmë juridike reciproke të shpejtë dhe efektive, tëmundësojnë kordinim dinjitoz në realizimin e hetimeve të përbashkëta, bashkëpunim në zbatimin e ligjit, transferimin e procedimeve penale si edhe të personave të dënuar duke shfaqur vullnet të qartë dhe të vendosurnë parandalimin dhe luftën e krimit.

22 Udhëzues u strategjisë për krimin e Organizuar, Kombet e Bashkuara Vjena 2021.

23 Joutsen,M. "*The European Union and Cooperation in Criminal Matters; the search for balance*," HRUNI, nr.25./2006

Angazhimi ligjor në trajtimin ekrimittëorganizuar.

Kompleksiteti dhe përhapia e vrullshme e krimit të organizuar gjatë dhjet viteve të fundit ka rritur pasigurin shoqërore. Është tentuar vashdimisht të zbehet kjo pasiguri nëpërmjet miratimit të ligjeve të reja ose ndryshimit të ligjeve funksionale duke, synuar përshtatijen e tyre me zhvillimet sociale, ekonomike dhe infrastrukturore.

Zhvillimet e fundit legjislative kanë reflektuar tendenc për të korrigjuar apo plotësuar mangësit ligjore, mirpo shpejtësia e zhvillimeve teknologjike dhe karakteri fluid[24] i krimit të organizuar kanë krijuar vazhdimisht vështirësi jo vetëm në rregullimin ligjor por edhe në hetimin e dinamikave të reja kriminale.

Në këtë pikë shqipëria ka bërë përpjekjet e veta, duke ofruar progres në fushën e reformave ligjore.Gjatë viteve të fundit Parlamenti Shqiptarë ka miratuar ligje, strategji dhe plane veprimi të diktuara nga nevoja e parandalimit dhe luftës kundër krimit në përgjithësi dhe formave të veçanta në veçanti. Pavarësisht nevojës së tyre jo gjithmonë këto nisma ligjore kanë garantuar zbatueshmëri efektiv.[25]

Reformat ligjore, përbëjnë një sfidë të rëndësishme sidomos në vendet ku identifikohen forma të zhvilluara të krimit të organizuar.

Nga praktia ka rezultuar se ndryshimet ligjore sidomos në fushën penale janë bërë me vonesë dhe nuk i kanë paraprirë nevojave[26]. Në këto kushte çdo reformë ligjore duhet të jetë e studiuar dhe me prespektiv afatgjatë në mënyrë që ti përgjigjet nevojave socialedhe të mos shmang zbatueshmërinë e saj. Çdo mekanizëm kombëtarë duke përfshirë edhe Shqipërinë ka detyrim të bëjë progres jo vetëm në hartimin por edhe në zbatimin e ligjeve dhe luftimin ndaj krimit të organizuar, forcimit të sistemit të drejtësisë dhe bashkëpunimit rajonal.[27]

Veç punës së vazhdueshme në nivel kombëtarë për shkak të karakterit ndërkombëtar dhe shumë-dimensional të krimit të organizuar diktohet nevoja

---

24 Zhilla.F, Lamallari. B, "*Vleresimi i Riskut të Krimit të Organizuar në Shqipëri*", Tiranë 2015, fq.95.
"*Evoluimi i Strukturave Kriminale të organizuara kriminale në Shqipëri*" Tiranë 2016. Fq.6.

25 Hysi.V, "*Ligji, Shoqëria dhe sistemi i drejtësisë penalë*", botim në revisten shkencore Jus& Justicia nr4/ 2010. Fq.33.

26 Hysi.V, "*Ligji, Shoqëria dhe sistemi i drejtësisë penalë*", botim në revisten shkencore Jus& Justicia nr4/ 2010. Fq.38.

27 Raporti i Komisionit Europian, "*Albania 2009 Progress Raport*", fq. 11-12.

përafrimit të legjislacioneve[28] dhe ngritjes së strukturave që mundësojnë një bashkëpunim real ndërmjet autoriteteve të shteteve të ndryshme.[29] Në kuadër të reformavë të vazhdueshme ligjore dhe harmonizimit të ligjit Shqipëria ka ratifikuar në vitin 2002 konventën e Kombëve të Bashkuara"Kundër krimit të Organizuar", MSA, si edhe Rezoluta dhe Rekomandime të BE dhe KE, të cilat orjentojnë dhe inkurajojnë luftimin dhe parandalimi e krimit tëorganizuar.

Prespektiva e Shqipërisë drejtë BE, duhet te fokusohet në programe politike dhe teknike që trajtojnë me përparësi të veçantë parandalimin dhe dënimin e krimit të organizuar si edhe të synoj përqasjen e standarteve dhe praktikave respektive me standartet e Kombeve të Bashkuara, rekomandimet e Këshillit të Europës, Direktivat e BE dhe standartet e tjera ndërkombëtare në këtë fushë.[30]

Harmonizimi i ligjit është një mjet që mundëson parandalimin dhe dënimin e krimit të organizuar me anë të një strukturë të përforcuar që realizuhet nëpërmjet bashkëpunimit ndërkombëtar. Ai garanton një rregullim ligjor mbikombëtaretë harmonizuar dhe siguron struktura monitoruesë në zbatimi e tyre,[31] gjë e cila përforconë efiçencën në realizimin e objektivave. Ky proces është domosdoshëm për të siguruar zbatimin efikas të politikave kundër krimit të organizuar, dhe konfirmimin e pushtetit kombëtarë, nëpërmjet rritjes së presionit ndaj krimit. Pra, zhvillim isistemit ligjorë kombëtar dhe harmonizimi e tij përmirësojnë dhe forcojnë pozitën e sistemit kombëtar por pavarësisht kësaj nuk arrin të parandalojë fenomenin e krimittë organizuar i cilireflekton një aktivitet të konsoliduar. Në këtë këndvështrimi strukturat kombëtarë në bashkëpunim me ato ndërkombëtare,duhet tregojnë vëmendje dhe kujdes të vazhdueshëm për ngritjen e strukturave përkatëse në ofrimin dhe mbrojtjen praktike dhe ligjore të politikave strategjike, në luftën kundër krimit.

Bibliografia

- KonventaeKombeve të Bashkuar, "*Kundër krimit të organizuar*

28 Udhëzues i strategjisë për krimin e Organizuar, Kombet e Bashkuara Vjena 2021.fq/1

29 Hoxha.A, "*Harmonizimi i legjislacionit penal në kuadrin e hapsirës Europiane*", botim në revisten shkencore Jus& Justicia nr4/ 2010. Fq.81.

30 Projekti Rajonal CARPO- "*Raporti mbi Gjendjen e Krimit të Organizuar dhe Krimit Ekonomik në Europën Juglindore*" Strasburg, gusht 2006 fq.5

31 Galdini, Xh, "*Përafrimi i legjislacionit në kuadër të integrimit europian*" botim në revisten shkencore Jus& Justicia nr4/ 2010. Fq.107.

ndërkombëtarë".

- Organized Crime in Europe", *Concepts, Patterns and Control Policies in European Union and Beyond, red*. Cyrille Fijnuat and Letizia Paoli, "Springer", Holandë 2004.
- Hysi.V, "*Kriminalogjia*", Tiranë 2010.
- Adamoli,S; Di Nikola, A; Savona. E etj, "*Organized crime around tha world*", Helsinki, 1998.
- Harring. J, "*E drejta Penale*" vol.1, Tiranë, tetor 2013.
- Dragoti.E , "*Psikologjia ligjore e krimit*", Tiranë.
- Muçi. SH. "*E drejta penale Pjesa e Përgjithshme*", Tiranë 2016.
- Strategjia për mbrojtjen kibernitike 2018-2020. Fq.3.
- Savona.E, "*Measuring organized crimi: An international prespective*", botuar në: "Forum on crime and society" vëllimi 5, nr.1, United Nations, New York, 2009.
- *Udhëzues i strategjisë për krimin e Organizuar*, Kombet e Bashkuara Vjena 2021.
- Projekti Rajonal CARPO- "*Raporti mbi gjendjen e krimit të organizuar dhe krimit ekonomik në Europën Juglindore*" Strasburg, Gusht 2006.
- Joutsen,M. "*The European Union and Cooperation in Criminal Matters; the search for balance*," HRUNI, nr.25/2006.
- Zhilla.F, Lamallari. B, "*Vleresimi i Riskut të Krimit të Organizuar në Shqipëri*", Tiranë 2015.
- Zhilla.F, Lamallari. B "*Evoluimi i Strukturave Kriminale të organizuara kriminale në Shqipëri*" Tiranë 2016.
- Raporti i Komisionit Europian, "*Albania 2009 Progress Raport*".
- Hysi.V, "*Ligji, Shoqëria dhe sistemi i drejtësisë penalë*", botim në revisten shkencore Jus& Justicia nr4/ 2010.
- Hoxha.A, "*Harmonizimi i legjislacionit penal në kuadrin e hapsirës Europiane*", botim në revisten shkencore Jus& Justicia nr4/ 2010.
- Galdini, Xh, "*Përafrimi i legjislacionit në kuadër të integrimit europian*" botim në revisten shkencore Jus& Justicia nr4/ 2010.

(https://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike).

https://sq.wikipedia.org/wiki/Krimet_kibernetike.

http://instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/krimet-dhe-drejt%C3%ABsia-penale/#tab2.

VOTIMI ELEKTRONIK MES DETYRIMIT PËR TË SIGURUAR VOTIMIN E SHTETASVE JASHTË SHQIPËRISË DHE RREZIKUT PËR MASHTRIME ZGJEDHORE.

VERA SHTJEFNI[1]

Fakulteti Drejtësisë, Universiteti i Tiranës.

vera.shtjefni@unitir.edu.al

LULZIM LELÇAJ[2]

Departamenti i Shkencave Juridike, Albanian University.

l.lelcaj@albanianuniversity.edu.al

Abstract

The right to vote, as a fundamental human right, is increasingly being influenced by technological developments. At all times, and in every country, the challenge has been, is and will be to ensure freedom, equality, secrecy, accuracy of the vote and the prevention of electoral fraud.

In the last parliamentary elections only 46.33%. of voters participated in the elections. More than 1.3 million voters living outside Albania do not have the opportunity to vote if they do not come to Albania. The Albanian economy benefits from billions of dollars a year from remittances. This contribution is multiplied if we consider the direct and indirect investments of Albanian citizens residing abroad. Since 1990, Albania has held 9 parliamentary elections, 8 elections for local government bodies, 2 constitutional referendums and many by-elections. Recently, electronic voting has been experimented with as a pilot project, but within polling stations.

Electoral fraud through technology is a challenge to face, as well

as computer, financial, banking fraud which are present and persistent, nowadays. It is entirely possible to improve the criminal provisions in Chapter X "Criminal Offenses Affecting Free Elections and the Democratic Election System", by providing for figures of electoral crimes specifically related to electronic voting. In order to effectively investigate electoral fraud, amendments to the Code of Criminal Procedure would be needed to include these crimes in the substantive jurisdiction of the Court against Corruption and Organized Crime (CACOC) (Article 75 / a). Involving law enforcement agencies, engaging financial, technological and human resources in joint inter-institutional task force groups would guarantee efficiency and effectiveness, as has happened in other countries.

Electronic voting should be an obligation for the Albanian government and state institutions to enable voters residing outside the territory of Albania to participate in the elections.

Key words: the right to vote, voters residing outside, electronic voting, electoral fraud, criminal offenses.

Hyrje.

Në demokracinë përfaqësuese qytetarët janë mbartës të sovranitetit dhe ushtrojnë pushtetin duke zgjedhur përfaqësuesit e tyre. Ushtrimi i të drejtës së zgjedhjes nga një numër sa më i madh qytetarësh është kontribut i drejtëpërdrejtë në forcimin e shtetit dhe legjitimitetin e organeve përfaqësuese. E drejta për të votuar, si një e drejtë themelore, po ndikohet gjithnjë e më shumë nga zhvillimet teknologjike. Në çdo kohë e vend sfida ka qenë, është dhe do të jetë sigurimi i lirisë, barazisë, fshehtësisë, saktësisë së votës dhe parandalimi i mashtrimit.

Në Shqipëri janë zhvilluar 9 zgjedhje parlamentare, 8 zgjedhje për organet e qeverisjes vendore, 2 referendume kushtetuese dhe shumë zgjedhje të pjesëshme. Pjesëmarrja në zgjedhje në Shqipëri ka pësuar rënie vit pas viti, pavarësisht se numri i qytetarëve me të drejtë vote është rritur. Në vitin 1991 Shqipëria ka patur afërsisht 1,984,933 votues dhe kanë marrë pjesë në zgjedhje rreth 1,963,568 votues. Në vitin 1992 ka patur afërsisht 2 milion votues dhe kanë marrë pjesë në zgjedhje rreth 1,826,142 votues. Në vitin 2005 nga 2 850 891 qytetarë me të drejtë vote kanë marrë pjesë në zgjedhje 1 403 473 votues. Në vitin 2009 nga 3 084 946 qytetarë me të drejtë vote kanë marrë pjesë në zgjedhje 1 519 176 votues. Në zgjedhjet parlamentare të vitit 2013, nga 3 271 885 qytetarë me të drejtë vote kanë marrë pjesë në

zgjedhje 1 744 261 votues[1]. Në vitin 2017 nga 3.452.324 qytetarë me të drejtë vote kanë marrë pjesë në zgjedhje 1.613.810 votues. Në zgjedhjet e fundit parlamentare të 25 prillit 2021, nga 3.588.869 qytetarë me të drejtë vote kanë marrë pjesë në zgjedhje 1.662 274 votues[2] (46.33%). Rënia e pjesëmarrjes në zgjedhje, pavarësisht se numri i qytetarëve me të drejtë vote është rritur, duket se ka si shkak kryesor faktin që një numër shumë i madh votuesish jetojnë jashtë Shqipërisë. Kjo konfirmohet me të dhënat e INSTAT, sipas të cilave 1.684.135[3] shqiptarë jetojnë jashtë Shqipërisë. Më shumë se 1.3 milion prej votuesve jashtë Shqipërisë nuk kanë mundësi të votojnë. Për shkak të emigracionit masiv Shqipëria ka specifikën që gati gjysma qytetarëve me të drejtë vote ndodhen jashtë territorit të saj dhe rënia e numrit të votuesve lidhet kryesisht me këtë fenomen.

Standartet ndërkombëtare lidhur me votimin elektronik.

Komiteti i Ministrave i Këshillit të Evropës, me Rekomandimin CM/Rec(2017)5 "Mbi standardet e votimit elektronik"[4] ka vendosur standarde ndërkombëtare në fushën e votimit elektronik. Ky rekomandim dhe dokumentet shoqëruese[5] përmbajnë aspektet thelbësore të votimit elektronik dhe trajtojnë përdorimin e mjeteve elektronike për hedhjen dhe numërimin e votave. Kjo kategori përfshin sisteme të tilla si, paisjet elektronike të votimit elektronik dhe sistemet e votimit në internet. Rekomandimi synon të harmonizojë zbatimin e parimeve të zgjedhjeve gjatë përdorimit të votimit elektronik.

Kodi i Praktikave të Mira të Komisionit të Venecias nuk e përjashton këtë alternativë, por kërkon që ky votim të përmbushë standardet demokratike të fshehtësise së votimit, sigurisë, besueshmërisë dhe integritetit të votimit. Kodi shprehet se: "Metodat e votimit elektronik duhet të jenë të sigurta dhe të besueshme. Ato janë të sigurta në rast se sistemi i reziston një sulmi të qëllimshëm; ato janë të besueshme në rast se mund të funksionojnë vetë pavarësisht nga ndonjë e metë në hardware ose software. Përveç kësaj,

1 Inter-Parliamentary Union http://archive.ipu.org/parline-e/reports/2001_arc.htm

2 https://kqz.gov.al/results/results2021/results2021.htm

3 http://www.instat.gov.al/media/7848/diaspora-ne-shifra-2020.pdf

4 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

5 Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. https://rm.coe.int/168071bc84
Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. https://rm.coe.int/1680726c0b

zgjedhësi duhet të jetë në gjendje të marrë konfirmim për votën e tij dhe, nëqoftëse është e nevojshme, t'a korrigjojë pa cënuar parimin e fshehtësisë së votës."[6].

Gjykata Evropiane e të Drejtave të Njeriut[7] e ka përsëritur pajtueshmërinë e imponimit të një kriteri vendbanimi me nenin 3 të Protokollit nr.1. Atë mund ta përligjin disa arsye: së pari, prezumimi se një qytetar jo me banim aty është i interesuar më pak drejtpërsëdrejti ose më pak për problemet e përditshme të vendit të tij, si edhe i njeh më pak ato; së dyti, kandidatët për zgjedhjet legjislative nuk kanë kurrfarë mundësie që t'ua paraqesin sfidat e ndryshme zgjedhore qytetarëve që ndodhen jashtë shtetit dhe këta të fundit kanë më pak ndikim në përzgjedhjen e kandidatëve apo në përcaktimin e programeve të tyre zgjedhore; së treti, lidhja e ngushtë ndërmjet së drejtës së votës në zgjedhjet legjislative dhe faktit që prekesh drejtpërdrejt nga aktet e organeve politike të zgjedhura në këtë mënyrë; dhe, së katërti, shqetësimi i drejtë që mund të ketë ligjvënësi për ta kufizuar ndikimin e qytetarëve me banim jashtë shtetit mbi zgjedhje që kanë të bëjnë me disa pika të cilat, ndonëse duke qenë themelore, prekin në radhë të parë personat që janë me banim brenda vendit.

Kushtetuta dhe legjislacioni zgjedhor shqiptar

Kushtetuta dhe legjislacioni zgjedhor[8] shqiptar parashikojnë ushtrimin vullnetar të të drejtës së votës dhe jo votimin e detyrueshëm[9]. Kodi zgjedhor

---

6 Kodi i praktikes se mire ne çeshtjet zgjedhore udhezime dhe raporti shpjegues Miratuar nga Komisioni i Venecias në Mbledhjen e tij 52-të Plenare (Venecia, 18-19 Tetor 2002), pika 43, fq.23. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev2-cor-alb

7 Udhëzues rreth nenit 3 të Protokollit nr. 1 të Konventës Evropiane të të Drejtave të Njeriut E drejta për zgjedhje të lira Përditësuar më 30 prill 2017§ 28-29 fq 10-11 https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_SQI.pdf

8 Kodi zgjedhor, në nenin 44, parashikon si kritere, përveç kushteve që lidhen me shtetësinë shqiptare, moshën 18 vjeç, qoftë edhe në datën e zgjedhjeve, të mos jetë shpallur me vendim gjyqësor të formës së prerë si i pazoti për të vepruar, kërkon që shtetasi shqiptar të jetë i regjistruar në Regjistrin Kombëtar të Gjendjes Civile dhe të ketë vendbanimin e regjistruar në territorin e një prej zonave të qendrave të votimit.

9 Shumica e shteteve demokratike e konsiderojnë pjesëmarrjen në zgjedhjet si e drejtë e zgjedhësve. Disa shteti e konsiderojnë atë edhe si përgjegjësi. Në disa prej këtyrë vendeve, votimi në zgjedhje është bërë i detyrueshëm dhe është rregulluar në kushtetutat kombëtare dhe ligjet zgjedhore. Ka shtete që shkojnë aq larg sa të vendosin sanksione ndaj votuesve që nuk marrin pjesë në votim. (burimi i informacionit The

njeh votimin në qendrat e votimit përmes prezencës fizike të zgjedhësit në adresën e tij në Shqipëri. Kodi Zgjedhor nuk njeh format e votimit në distancë (votimin përmes internetit apo votimin me postë). Qytetarët shqiptarë, përfshirë edhe ata që ndodhen jashtë territorit të Shqipërisë, mund ta ushtrojnë të drejtën e tyre vetëm nëse paraqiten në qëndrën e votimit në zonën zgjedhore ku kanë adresën në Shqipëri. Numri i votuesve që e ushtrojnë këtë të drejtë ka qenë i kufizuar. Sipas ligjit nr.9034/2003 "Për emigrimin e shtetasve shqiptarë për motive punësimi", shteti garanton përkujdesjen dhe mbrojtjen e shtetasve të tij emigrantë, si dhe ruajtjen dhe forcimin e lidhjeve të tyre me Republikën e Shqipërisë.(neni 1, pika 2) . Shteti krijon lehtësi për emigrantët që kthehen në atdhe për të ushtruar të drejtën e votës në zbatim të Kodit Zgjedhor. (neni 5, pika 2). Deri më sot ky angazhim nuk është përmbushur në asnjë rast. Ministria e Diasporës pranon së "Kodi Zgjedhor ka përjashtuar çdo mundësi për proces të zhvilluar jashtë vendit, pasi specifikon "votimin në territorin e vendit". Ky specifikim i lë pa vlerë, në praktikë, dispozitat e "Ligjit për Emigrimin…", i cili përcakton detyrimin e autoriteteve përgjegjëse për të krijuar lehtësitë për votimin e migrantëve. ... Kuvendi duhet të vlerësojë faktin që Kushtetuta e Republikës së Shqipërisë parashikon të drejtën e çdo shtetasi që të zgjedhë dhe të zgjidhet. Ky parim universal nuk ka gjetur konkretizimin e vet në Kodin Zgjedhor të vendit, i cili praktikisht nuk u krijon mundësinë shtetasve shqiptarë që banojnë në një shtet tjetër të votojnë për zgjedhjet e përgjithshme legjislative apo në referendumet kombëtare në Shqipëri."[10]

Për më tepër, ka patur pretendime nga subjekte zgjedhore apo kandidatë, që për disa prej këtyre zgjedhësve është organizuar dhe financuar udhëtimi, me qëllim pjesëmarrjen në votim nga kandidatë apo subjekte politike të interesuara, duke aluduar për votim jo të lirë e të fshehtë.

Diskutimi në rastin e Shqipërisë është nëse qytetarët shqiptarë që jetojnë në shtete të tjera do të kenë mundësi të votojnë nga vendet ku jetojnë, dhe nëse ata do të votojnë në zonën zgjedhore ku janë të regjistruar në Shqipëri, apo do të duhej të përcaktohej një zonë zgjedhore e veçantë me një numër të caktuar deputetësh. Në pamundësi për të zgjeruar objektin e punimit në këto dy çështje, është evidente që qytetarët shqiptarë me banim në shtete të tjera

International Institute for Democracy and Electoral Assistance - International IDEA) https://www.idea.int/data-tools/data/voter-turnout/compulsory-voting

10 Ministri i Shtetit pwr Diasporwn. "Votimi i shtetasve të republikës së shqipërisë jashtë vendit" Informacion për Komisionin e Reformës Zgjedhore në Kuvendin e Shqipërisë' fq.5. https://diaspora.gov.al/wp-content/uploads/2018/07/VOTIMI-I-SHTETASVE-TE-REPUBLIKES-SE-SHQIPERISE-JASHTE-VENDIT.pdf

ruajnë një lidhje jashtëzakonisht të fortë me shtetin e tyre dhe kanë kontribut thelbësor në zhvillimin ekonomik, social, kulturor dhe politik të vendit tonë në këto 30 vite. Remitancat[11] kanë qenë një ndër shtytësit më të mëdhënj të ekonomisë shqiptare gjatë këtyre 30 viteve[12]. Këta qytetarë janë integruar në shoqëritë perëndimore, duke marrë vlerat më të mira të qytetërimit perëndimor, zhvillimit human si dhe pjesëmarjes në jetën demokratike. Vota e tyre do të ishte një kontribut i shtuar në dëmokracinë përfaqësuese dhe do të rriste legjitimitetin e të zgjedhurve. Çështja nuk duhet të jetë a duhet, por si mund të realizohet menjëherë votimi i tyre në zgjedhjet më të afërta. Përdorimi i teknologjisë është një alternativë për votimin e qytetarëve shqiptarë pa patur nevojë të paraqiten në qendrën e votimit, sikurse kryejnë një pjesë jo të vogël të aktivitetit të përditshëm përmes shërbimeve elektronike. Si në çdo fushë të jetës, përdorimi i teknologjisë ka avatazhet e padiskutueshme dhe rrisqet e veta.

Krijimi i kushteve për të votuar në zgjedhje për qytetarët me banim jashtë territorit të shtetit, ka qenë sfidë për shumë shtete demokratike. Tradicionalisht janë përdorur alternativa votimi si (votimi me postë, apo votimi pranë ambasadave apo në konsullata, në shtetin ku jetojnë). Problematika e vendit tonë është shumë më e madhe pasi vështirë të gjendet një shtet ku gati gjysma e votuesve të tij të jetojnë jashtë vendit dhe të mos kenë mundësi reale të votojnë.

Teknologjia mund të përdoret si një mjet i fuqishëm për të drejtat e njeriut. Zhvillimet teknologjike kanë sjellë një realitet të ri për ushtrimin e të drejtën së votës. Votimi ka përparuar në teknologji nga ditët tradicionale kur votuesit hidhnin votat e shënuara në një guaskë, copë qeramike ose kartë në një kuti deri në ditët aktuale ku votimi kontrollohet nga elektronika dhe proceset që çojnë në votim mbeten të padukshme për syrin e njeriut. Pavarësisht ndryshimit në metodën e votimit, aspektet bazë të taktikave të mira të votimit mbeten të njëjta: sigurimi i një vote për votues, ruajtja e anonimitetit të votuesve, saktësia e votës, siguria e sistemit dhe parandalimi i mashtrimit[13].

11 Banka e Shqipërisë "Pandemia dhe Remitancat" https://online.fliphtml5.com/wpfxe/bbph/#p=4

12 Sipas të dhënave zyrtare nga Banka e Shqipërisë remitancat në vitin 2021 arritën në 761 milionë euro, 13% më shumë se në vitin 2020. Shifra reale e remitancave është shumë më e madhe për shkak se një pjesë e fluksit të remitancave nuk kalojnë domosdoshmërisht përmes transksioneve bankare. Një në katër familje marrin të ardhura nga emigrantët, para që janë burimi i vetëm i jetesës për pjesën dërrmuese të tyre. Janë gjithsej 220 mijë familje që jetojnë me këto të ardhura, në pamundësi të një burimi tjetër

13 https://cs.stanford.edu/people/eroberts/cs201/projects/2006-07/electronic-voting/

Shembujt se si teknologjia mund të përdoret si një mjet i fuqishëm për të drejtat e njeriut po zgjerohen gjithnjë e më shumë. Teknologjitë më të reja si inteligjenca artificiale, automatizimi dhe blockchain kanë potencialin për të dhënë kontribut të rëndësishëm pozitiv në promovimin dhe mbrojtjen e të drejtave të njeriut[14].

Përfshirja e teknologjisë në sistemin zgjedhor në Shqipëri.

Hapi i parë i përfshirjes së teknologjisë ka qenë regjistri elektronik i shtetasve. Prej këtij regjistri u mundësua nxjerrja e listave të zgjedhësve nga zgjedhjet e përgjithshme të vitit 2009 e në vijim. Më vonë është bërë identifikimi i zgjedhësve përmes dokumentave biometrike (karta identiteti ose pasaportave biometrike, zgjedhjet vendore te vitit 2011). Në vitin 2013, KQZ në Shqipëri aprovoi projektin qe parashikohej si pilot në Qarkun e Fierit për numërimin elektronik të votave për zgjedhjet parlamentare të 2013, gjithashtu në Tirane parashikohej aplikimi i projektit te identifikimit elektronik të votuesve, duke parashikuar kontrollin e kartave të identitetit në mënyrë elektronike. Këto projekte nuk arritën të zbatohen për shkak të disa problemeve teknike. Në zgjedhjet e vitit 2015 e 2017 nuk është aplikuar votim elektronik as si projekt pilot. Hapi më serioz në implementimin e teknologjisë ka qenë pilotimi i votimit elektronik brenda qendrave të votimit, realizimi i të cilit u bë vetëm në zgjedhjet e përgjithshme të vitit 2021.Votimi dhe numërimi elektronik është përdorur në mënyrë të kufizuar në zgjedhjet parlamentare të vitit 2021 në një zonë të administrimit zgjedhor, si dhe në zgjedhjet e pjesëshme vendore në vitin 2022, në bashkinë Vorë. Në të gjitha rastet është përdorur votimi elektronik me paisje të vendosura në qëndrat e votimit.

Votimi në distancë nuk është shqyrtuar deri më sot në Shqipëri. Edhe në rastet e diskutimit të mundësisë së votës të zgjedhësve shqiptarë që nuk jetojnë në Shqipëri, diskutimi ka mbetur në deklarata të përgjithshme nëse duhet të ketë një zonë zgjedhore të posaçme për këta zgjedhës me një numër të caktuar deputetësh dhe cila prej alternativave të votimit do të përdorej ndërmjet votimit në përfaqësitë diplomatike, votimit me postë, ku kërkohej nga këta votues të shpehin interes për të marrë pjesë në zgjedhje, të deklarojnë adresën ku jetojnë dhe procedura në vijim. Ky process nuk ka nisur. Në faqen zyrtare të KQZ rubrika "Rregullat për votimin jashtë vendit" theksohet se"Kodi Zgjedhor i Republikës së Shqipërisë garanton të drejtën e zgjedhësve shqiptarë që kanë vendbanimin e përhershëm jashtë territorit të Republikës së Shqipërisë të votojnë në zgjedhjet parlamentare.

index_files/page0002.html

14 Open global rights https://www.openglobalrights.org/technology/

Avantazhet dhe dizavantazhet e votimit elektronik.

Votimi elektronik ka mbështetësit dhe kundërshtarët e tij në të gjithë shtetet ku është aplikuar apo tentohet të zbatohet[15]. Pavarësisht nga specifikat e shteteve, pranohet se votimi elektronik është më i lehtë. Votimi elektronik mundëson të votosh nga çdo vend, në çdo kohë pa patur nevojë të shkosh në qendrën e votimit ose në kutinë postare për të dërguar fletën e votimit. Votuesit jashtë vendit kanë mundësi të votojnë në të njëjtat kushte dhe vota e tyre nuk vonon të shkojë në komisionin e numërimit sikurse mund të ndodhë kur voton me postë. Votimi elektronik ka më pak pengesa për të votuar[16]. Me këtë votim më shumë qytetarë e ushtrojnë këtë të drejtë. Të rinjtë, të cilët tradicionalisht votojnë më rrallë, ka më shumë të ngjarë të jenë të interesuar të përfshihen nëpërmjet votimit elektronik. Në votimin elektronik nuk ka vota të pavlefshme të shkaktuara nga gabimet e bëra në fletën e votimit. Asnjë sistem votimi nuk është 100% i sigurt, as i pagabueshëm.[17]

Në vendet ku është aplikuar (Estoni, Zvicër) është e provuar së votimi në internet ka rritur dukshëm pjesëmarrjen në votime të qytetarëve me banim jashtë vendit. Ai ka një efekt edhe më të theksuar në pjesëmarrjen e votuesve emigrantë në kontekste ku emigrantët nuk mund të votojnë me postë, por duhet të votojnë personalisht. Megjithatë, mbetet e paqartë se deri në çfarë mase votimi në internet rrit pjesëmarrjen në zgjedhje[18]

Si disavantazhe të votimit elektronik konsiderohen mosgarantimi i plotë i fshehtësisë së votës; rreziku i manupulimit të zgjedhjeve dhe votave përmes hakerimit, blerjes së votave dhe manipulime të tjera[19]. Ka patur raste të sulmeve kibernetike nga kriminelët, shërbimet e huaja të inteligjencës apo kompanitë, të cilët kanë ngritur dyshime për manipulim të votave apo zgjedhjeve[20]. Janë ngritur shqetësime mbi rreziqe që lidhen me veprime

15 Në Gjermani Gjykata Kushtetuese ka konsideruar këtë votim si antikushtetues.

16 Introducing Electronic Voting: Essential Considerations Policy Paper. December 2011 fq.8. International IDEA Publications Office ISBN: 978-91-86565-21-3

17 https://www.swissinfo.ch/eng/electronic-voting_ten-arguments-for-and-against-e-voting/43959200

18 Micha Germann. Internet voting increases expatriate voter turnout. https://www.sciencedirect.com/science/article/abs/pii/S0740624X20303397?via%3Dihub

19 Introducing Electronic Voting: Essential Considerations Policy Paper December 2011 fq.9. International IDEA Publications Office ISBN: 978-91-86565-21-3

20 https://www.swissinfo.ch/eng/electronic-voting_ten-arguments-for-and-against-e-voting/43959200

njerëzore[21] dhe me rreziqet të lidhura me teknologjinë[22]

Studimet kanë treguar se zbatimi i votimit elektronik zvogëlon rrezikun e mashtrimit dhe manipulimit të gjerë në nivel qendre votimi, por përqendron rrezikun e manipulimit në nivelin qendror; Nuk është i mundur rinumërimi, ndryshe nga fletëvotimet fizike, votat elektronike nuk mund të numërohen manualisht. Qytetarët duhet t'i besojnë verbërisht sistemit të votimit elektronik; Votimi elektronik është i shtrenjtë. Kundërshtarët argumentojnë se kostot e votimit elektronik janë abuzive[23].

Modele të suksesshme të zbatimit të Votimit elektronik përmes internetit.

Estonia është një shëmbull ku votuesit zgjedhin liderët e tyre përmes votimit në internet dhe sistemet e ndërtuara mirë mund t'i ofrojnë komoditet

21 Mungesa e aftësive teknike të përshtatshme për votuesit për të përdorur votimin në distancë të internetit; Mungesa e aftësive teknike të duhura për sa i përket zyrtarëve zgjedhorë, duke çuar në situatën kur ata mund të humbasin kontrollin mbi procesin e votimit në internet; qytetarët nuk mund të sigurojnë se vota e tyre mbetet e fshehtë; Mungesa e transparencës kur votuesit nuk mund të jenë të sigurt nëse votat e tyre janë numëruar dhe ruajtur saktë; rreziku i ndërhyrjes nga dikush tjetër në afërsi të një votuesi (për shembull, në shtëpi ose në punë) gjatë procesit të votimit në distancë në internet për të kontrolluar vendimet e votimit nëpërmjet frikësimit, mashtrimit, detyrimit për të shitur votën etj.; Rreziku që votuesit që nuk kanë akses në internet do ta ndjejnë veten të diskriminuar nëse votimi në distancë në internet është i vetmi opsion për të votuar"
European Parliament. Potential and challenges of e-voting in the European Union fq.16
https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf

22 "ndarja dixhitale - mundësitë e pabarabarta të aksesit në internet midis grupeve të ndryshme sociodemografike; si rrjedhojë rreziku që votuesit e internetit të mos përfaqësojnë elektoratin e përgjithshëm, por vetëm një pjesë të tij, duke shtrembëruar rezultatet e votimit në favor të grupeve të caktuara; Mundësia e sulmit ose prishjes së sistemit, ose dështimi i lidhjes; Mundësia që kompjuterët personalë të votuesit janë të infektuar me viruse ose malware, gjë që, nga ana tjetër, mund të rezultojë në shtrembërim të vendimit të votimit ose/dhe të ndikojë në të gjithë sistemin e votimit në internet; kompleksiteti me identifikimin e saktë të votuesit; sigurimi i transparencës së tabelave; Sigurimi i masave parandaluese kundër votimit të shumëfishtë; Kompleksiteti me rinumërimin e votave sipas kërkesës së kandidatëve në rastin e rezultateve shumë të afërta të zgjedhjeve"
European Parliament. Potential and challenges of e-voting in the European Union fq.17
https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf

23 https://www.swissinfo.ch/eng/electronic-voting_ten-arguments-for-and-against-e-voting/43959200

votuesit, duke respektuar parimet themelore demokratike të fshehtësisë dhe drejtësisë. Në Estoni, votuesit zgjedhin liderët e tyre përmes votimit në internet. Vendi po ndërmerr hapa për të shmangur sulmet e mundshme të hakerimit ndërsa frika nga siguria kibernetike intensifikohet[24]. Votimi në internet u prezantua si një kanal votimi shtesë në vitin 2005 dhe gëzoi besim të gjerë që në fillim. Estonia gëzon një nivel të lartë besimi në institucionet e saj dhe votimi elektronik shoqëroi një program më të gjerë të dixhitalizimit të institucioneve të saj. As sulmet masive të hakerimit kundër infrastrukturës së qeverisjes elektronike të Estonisë përpara zgjedhjeve të vitit 2007 nuk e minuan këtë besim.[25] Votimi online në Estoni ka tre faza: regjistrimi dhe vërtetimi i votuesve; transmetimin e sigurt të votave në një kuti votimi virtuale dhe mbrojtjen e tyre pasi të kenë mbërritur; verifikimin që votat janë hedhur saktë. Ky sistem është i paisur me masa mbrojtëse të integruara për të minimizuar rreziqet në të tre fazat.[26] Estonia ka zhvilluar tetë zgjedhje mbarëkombëtare duke përdorur sistemin e votimit në internet. Në zgjedhjet parlamentare të 2015-ës, mbi 30 për qind e elektoratit zgjodhën të votonin në internet në vend që të vizitonin një qendër votimi. Në disa sondazhe, deri në 20 për qind e votuesve të Estonisë në internet thonë se nuk do të kishin votuar nëse nuk do të ishin në gjendje ta bënin këtë në internet. Sistemi i votimit në internet i Estonisë nuk ka pësuar kurrë një shkelje të sigurisë ose nuk ka prodhuar një numërim të gabuar.

Sistemi mundëson që votuesi të informohet që fleta e votimit ka arritur në kutinë e votimit e paprekur. Pas votimit sistemi gjeneron një faturë unike votimi që shfaqet si një kod QR në laptop. Votuesi më pas mund të skanojë kodin QR duke përdorur një aplikacion smartphone, i cili shfaq përmbajtjen e votës që është regjistruar në server. Votuesi mund të shohë lehtësisht se vota e tij u hodh me sukses dhe saktë[27]. Megjithatë ka edhe vlerësime që kundërshtojnë aplikimin e këtij sistemi. Sipas një analize të bërë këtij sistemi është arritur në përfundim se: "një sulmues i nivelit shtetëror, kriminel i sofistikuar ose i brendshëm i pandershëm mund të mposhte si kontrollet teknologjike ashtu edhe ato procedurale për të manipuluar rezultatet

24 https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber-defences/

25 Introducing Electronic Voting: Essential Considerations Policy Paper December 2011 fq.18. International IDEA Publications Office ISBN: 978-91-86565-21-3

26 Electronic Voting Committee. General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia. Document: IVXV-ÜK-0.98 Date: 23 May 2016. https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf

27 https://spectrum.ieee.org/online-voting-isnt-as-flawed-as-you-thinkjust-ask-estonia

e zgjedhjeve. … nëse nuk do të ketë përparime thelbësore në sigurinë kompjuterike, profili i rrezikut mund të jetë më i favorshëm për votimin në internet, por ne nuk besojmë se sistemi I-voting mund të bëhet i sigurt sot.... ... Shumë estonezë mbështesin I-votën sepse besojnë se ka një mashtrim të përhapur në sistemin e bazuar në letra të vendit"[28].

Në Shqipëri është e mundur që të implementohet votimi elektronik, krahas votimit tradicional. Zhvillimet teknologjike e mundësojnë një gjë të tillë. Infrastruktura dixhitale është zhvilluar, është rritur aksesi i qytetarëve ndaj teknologjisë dixhitale dhe internetit. Megjithatë duhet të jemi të qartë se përdorimi i teknologjisë nuk është "instrumenti magjik" për të zgjidhur të gjithë problematikën zgjedhore. Mashtrimet zgjedhore apo aktet e tjera të paligjshme nuk eleminohen nga votimi elektronik. Vështirë të besohet se votimi elektronik do të eleminonte shitblerjen e votës, intimidimin e votuesve, korrupsionin zgjedhor, financimet e paligjshme apo implikimet e botës së krimit. Studime serioze kanë përforcuar idëne se teknologjitë e reja të votimit ... mund të luajnë një rol në reduktimin e rasteve të mashtrimit, sepse ato kufizojnë përfshirjen njerëzore në procesin e votimit dhe numërimit.[29] Edhe në SHBA ku ka kundërshti të forta për aplikimin e teknologjisë në votim, ekspertët bien dakord se nëse vetëm divizioni i teknologjisë zgjedhore .... do t'i përmbushte detyrat e tij me aq përgjegjësi sa departamentet e tjera të asaj agjencie të shquar, perspektivat për votim në internet në SHBA do të ishin të shkëlqyera.[30] Sfida mbetet që sistemi i votimit përmes internetit të krijojë besim, dhe kjo kërkon besimin e zhvilluesve të softuerit që krijojnë sistemin, besimin tek ofruesit e rrjetit, besimin në protokollet e rrjetit dhe besimin në sistemet përfundimtare në shtëpitë e njerëzve.[31]

Shqipëria është në kohën e duhur për ta ndërmarrë këtë hap - 3 vite

---

28 Drew Springall; Travis Finkenauer; Zakir Durumeric; Jason Kitcat; Harri Hursti; Margaret MacAlpine; J. Alex Halderman. Security Analysis of the Estonian Internet Voting System fq.11. https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

29 Max Bader, Do new voting technologies prevent fraud? Evidence from Russia. Usenix Journal of Election Technology and Systems (JETS) Volume 2, Number 1 • December 2013 https://www.usenix.org/system/files/jets/issues/0201/jets_0201-bader.pdf

30 William J. Kelleher. Internet Voting in the USA: History and Prospects; fq.35. https://www.eac.gov/sites/default/files/eac_assets/1/28/William-Kelleher-Internet-Voting-WPSA-Paper-July-9th.pdf

31 Aviel Rubin. Professor of computer science at Johns Hopkins University and the technical director of the Johns Hopkins University Information Security Institute. https://engineering.jhu.edu/magazine/2016/06/internet-voting-nonstarter/#.YrBLC3ZByMo

janë më se të mjaftueshme për të ndërtuar infrastrukturën, për të testuar funksionimin e saj, për të krijuar mekanizmat institucionale (task force) si dhe për të ndërmarrë përmirësimet e nevojshme legjislative. Rreziqet që mund të sjellë votimi elektronik në Shqipëri janë plotësisht të parandalueshme nëse ka vullnet nga institucionet shtetërore, subjektet zgjedhore dhe agjencitë e zbatimit të ligjit. Për shkak të kompleksitetit dhë rëndësisë do të duhej të ngrihej një strukturë e posaçme për të realizuar këtë votim. Modeli estonez sugjeron krijimin e një Komiteti për Votimin Elektronik[32], i cili do të duhej të jetë pjesë e strukturës së Komisionit Qendror të Zgjedhjeve.

Për të goditur mashtrimet zgjedhore gjatë përdorimit të votimit elektronik do të jetë e nevojshme të miratohen shtesa dhe ndryshime në Kodin Penal dhe Kodin e Procedurës Penale. Kodi Penal i Shqipërisë ka parashikuar veprat penale në fushën e zgjedhjeve në një kre të veçantë[33] Amendimet gjatë viteve të dispozitave kanë qenë pjesë e paketës të reformave zgjedhore bashkë me Kodin Zgjedhor. Ndërhyrjet më të rëndësishme janë bërë 10 vite me parë me ligjin Nr. 23/2012, me ndryshimet në vitin 2017 e 2020. Parashikimi i figurave të veprave penale në fushën e zgjedhjeve lidhet më së shumti me pretendimet e subjekteve zgjedhore apo gjetjet e raporteve të OSBE/ODHIR.

Karakteristikë e këtyre ndryshimeve ka qenë kriminalizimi i disa veprimeve shoqërisht të rrezikshme dhe të kundërligjshme të konstatuara në fushën e zgjedhjeve dhe ashpërsimi i sanksioneve penale për figura ekzistuese. Amendimet e Kodit Penal kanë ardhur nga konsensusi mazhorancë-opozitë. Ndryshimet e Kodit Penal nuk janë paraprirë apo shoqëruar me një analizë vlerësuese të efikasitetit të kuadrit ligjor penal në fuqi dhe zbatueshmërisë së tij, për të dalë në përfundimin e nevojës për përmirësime të kuadrit ligjor ekzistues. Mungesa e një vlerësimi të tillë ka sjellë situatën që të mos përcaktohet nëse problematika shkaktohet nga moszbatimi i ligjit apo nga mangësitë ligjore.

Dispozitat e veprave penale në fushën e zgjedhjeve kriminalizojnë akte penalisht të dënueshme që lidhen me procesin zgjedhor dhe votimin tradicional. Neni 326 parashikon falsifikimin, shpërndarjen ose përdorimin e fletëve të votimit, të dokumenteve dhe materialit zgjedhor me qëllim

32 Në këtë strukturë do të duhej të merrnin pjesë ekspertë ligjor të zgjedhjeve, ekspertë të fushës informatike, të cilët gëzojnë besimin e institucioneve shtetrore dhe subjekteve zgjedhore (përsa kohë sistemi zgjedhor në Shqipëri funksionon mbi bazën e balancimit në përfaqësim të subjekteve zgjedhore).

33 Kreu X. “ Vepra penale që prekin zgjedhjet e lira dhe sistemin demokratik të zgjedhjeve”.

ndryshmin e rezultatit të zgjedhjeve nëpërmjet paraqitjes në to të të dhënave, që dihen se janë të pasakta, zëvendësimi i të saktave me të rreme ose nëpërmjet futjes në kuti të fletëve të votimit në mënyrë të paligjshme. Si rrethana rënduese parashikohet kur kjo vepër penale kryhet nga personat që kanë për detyrë të administrojnë procesin zgjedhor, ose ka sjellë pasoja të rënda në mbarëvajtjen e votimit, ka cenuar integritetin e rezultatit të zgjedhjeve apo ka sjellë pavlefshmërinë e tyre. Neni 326/a parashikon dëmtimin, prishjen, shkatërrimin me dashje, apo zëvendësimin në kundërshtim me ligjin i pajisjeve, vulave, kodeve të sigurisë apo çdo materiali tjetër zgjedhor të parashikuar nga ligji. Si rrethana rënduese parashikohet kur kjo vepër penale kryhen nga personat përgjegjës për administrimin zgjedhor ose në bashkëpunim, ose më shumë se një herë, apo kur kanë sjellë pasoja të rënda në mbarëvajtjen e zgjedhjeve, kanë sjellë pavlefshmërinë e tyre apo kanë cenuar rezultatin e votimit, dënohen me burgim nga tre gjer në tetë vjet. Neni 327 parashikon Shkeljen e rregullave që garantojnë fshehtësinë e votimit nga ana e zgjedhësit, nëpërmjet fotografimit të fletës së votimit, ose filmimit të saj, ose dokumentimit me çdo mjet dhe formë të mënyrës sesi ka votuar, shfaqjes së tyre tek persona të tjerë si dhe rrethanat rënduese kur Shkelja e rregullave që garantojnë fshehtësinë e votimit kryhet nga ana e personave të ngarkuar me zgjedhjet si dhe rrethanën rënduese të nxitjes me ose pa shpërblim, ose detyrimin e zgjedhësit për të shkelur rregullat që garantojnë fshehtësinë e votimit. Neni 330 parashikon pengimin e zgjedhësit për të votuar në qendrën e tij të votimit, duke shkelur rregullat e votimit, duke i marrë apo dëmtuar dokumentin e tij të identifikimit, apo në çdo formë tjetër, si dhe rrethanat rënduese kur kjo vepër kryhet më shumë se një herë, ndaj më shumë se një zgjedhësi apo kur kryhet nga komisionerët zgjedhorë. Neni 330/a parashikon braktisjen e detyrës apo refuzimin për të kryer detyrën nga personat e ngarkuar me administrimin e procesit të votimit dhe të numërimit si dhe rrethanat rënduese kur veprimet e mësipërme kryhen duke marrë me vete ose duke zhdukur materialet zgjedhore, ose kur kanë sjellë pasoja të rënda për procesin e votimit apo kanë çuar në pavlefshmërinë e zgjedhjeve. Neni 331 parashikon mospërfshirjen me dashje në listat e zgjedhësve të personave që e kanë të drejtën e zgjedhjes ose regjistrimi me dashje në to i personave që nuk e kanë këtë të drejtë si dhe rrethanat rënduese kur vepra penale kryhet në bashkëpunim, kur ka sjellë pasoja të rënda për interesat e zgjedhësve apo mbarëvajtjen e procesit zgjedhor. Neni 331/a parashikon marrjen ose përdormin e paligjshëm të dokumenteve të identifikimit të zgjedhësve.

Pjesa më e madhe e Veprave Penale në këtë kre janë të ngjashme me

vepra penale në krerët e tjerë, por dallojnë tek objekti i figurës së veprës penale dhe tek qëllimi kriminal, si element i anës subjektive. Legjislatori i ka parashikuar këto vepra, edhe pse figura të ngjashme ndodhen në krerë të tjerë, sepse ka synuar të mbrojë specifikisht sistemin demokratik të zgjedhjeve dhe zgjedhjet e lira dhe të theksojë si element qëllimin kriminal që ka subjekti aktiv i këtyre veprave.

Në asnjë dispozitë nuk është parashikuar vepër penale që të sanksionojë penalisht akte shoqërisht të rrezikshme dhe të kundërligjshme që lidhen me votimin elektronik apo keqpërdorimin e teknologjisë në zgjedhje, megjithëse përfshirja e teknologjisë në zgjedhje ka filluar gradualisht prej zgjedhjeve të vitit 2009 e vijim.

Në Kodin Penal janë parashikuar veprat penale të mashtrimit kompiuterik (Neni 143/b), Falsifikimi kompjuterik (Neni 186/a), Hyrja e paautorizuar kompjuterike (Neni 192/b), Në seksionin "Vepra penale kundër rendit dhe sigurisë publike" janë parashikuar veprat penale si: Përgjimi i paligjshëm i të dhënave kompjuterike (Neni 293/a), Ndërhyrja në të dhënat kompjuterike (Neni 293/b), Ndërhyrja në sistemet kompjuterike (Neni 293/c), Keqpërdorimi i pajisjeve (Neni 293/ç).

Megjithatë, këto dispozita nuk mund të aplikohen në rastet kur subjektet kryejnë një ndër veprat penale që cënojnë sistemin e zgjedhjeve me qëllim për të cënuar sistemin zgjedhor, të drejtën e votës apo zgjedhjet demokratike sepse objekti që cënohet në këtë rast janë marrëdhënjet juridike që janë vendosur për të mbrojtur sistemin demokratik të zgjedhjeve dhe zgjedhjet e lira. Sikurse për veprat e tjera penale në këtë kre, do të duhet te parashikohen veprat penale që lidhen me votimin elektronik. Amendimet e dispozitave penale do të jenë të lidhura ngushte me modelin e votimit elektronik që do të adoptohet në infrastrukturën zgjedhore. Do të jetë e nevojshme të parashikohen element specifikë që lidhen me anën objektive veprime/mosveprime kirminale, mjetet, menyrën vendin e kryerjes së veprës penale si dhe elementë të anës subjektive që lidhen më së shumti me përcaktimin e qëllimit kriminal për të ndikuar në rezultatin zgjedhor. Sanksionet penale do të duhet të jenë të ashpra, pasi rrezikshmëria e këtyre veprave penale është shumë e madhe për shkak të objektit që cënojnë dhe pasojat e rënda që sjellin.

Propozimet për amendimin e Kodit Penal në kreun X "Vepra penale që prekin zgjedhjet e lira dhe sistemin demokratik të zgjedhjeve".

Neni 326/b

Ndërhyrjet e paligjshme në sistemin elektronik të votimit.

Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike të sistemit elektronik të votimit apo ndërhyrja në funksionimin e sistemit kompjuterik të identifikimit të zgjedhësve, votimit elektronik ose nxjerrjes së rezultatit të votimit, me qëllim ndryshmin e rezultatit të zgjedhjeve, dënohen me burgim nga tre deri në dhjetë vjet.

Po këto vepra kur kryhen nga personat përgjegjës për administrimin e sistemit të votimit ose në bashkëpunim, ose më shumë se një herë, apo kur kanë sjellë pasoja të rënda në mbarëvajtjen e zgjedhjeve, kanë sjellë pavlefshmërinë e tyre apo kanë cenuar rezultatin e votimit, dënohen me burgim nga pesë deri në pesëmbëdhjetë vjet.

Neni 326/c

Ndërhyrja në sistemet kompjuterike të votimit

Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e sistemit kompjuterik të votimit elektronik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

Neni 326/ç

Ndërhyrja në të dhënat kompjuterike të zgjedhjeve

Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike të zgjedhjeve dënohen me burgim nga pesë deri në pesëmbëdhjetë vjet.

Neni 326/d/b

Keqpërdorimi i pajisjeve

Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në kreun X të këtij Kodi, dënohen me burgim nga tre

deri në shtatë vjet.

Propozime për amendime në Kodin e Procedurës Penale

Krimet zgjedhore duhet të jenë në Kompetencë lëndore të Gjykatës kundër Korrupsionit dhe Krimit të Organizuar për të rritur eficëncën e goditjes së krimit zgjedhor të natyrës kibernetike. Për këtë nevojitet amendimi i nenit Neni 75/a të Kodit të Procedurës Penale, Kompetencat e Gjykatës kundër Korrupsionit dhe Krimit të Organizuar, konkretisht përfshirjen e këtyre neneve në pikën a) të këtij neni.

Për shkak se krimet kompjuterike kryhen edhe nga jashtë, duhet të verifikohet nëse duhen përmirësime në legjislacionin e Shqipërisë, duke vlerësuar nëse instrumentet ligjore aktualë janë të mjaftueshëm apo duhet ndërhyrje në legjislacionin që parashikon bashkëpunimin juridiksional dhe ndihmës së ndërsjelltë gjyqësore me shtetet e huaja.

Konkluzione

Krijimi i kushteve për votimin e qytetarëve shqiptarë me banim jashtë vendit do të duhet të rezlizohet në zgjedhjet më të afërta dhe në çdo rast në zgjedhjet e ardhshme parlamentare. Votimi përmes internetit do të ishte një alternativë shumë e mirë për pjesëmarrjen në zgjedhje të këtyre votuesve.

Zhvillimet teknologjike mundësojnë përmbushjen e standardeve dhe parimet e zgjedhjeve të lira, të barabarta, të fshehta dhe të përgjithshme. Koha për të ndërtuar këtë sistem është e mjaftueshme dhe kostoja është e justifikueshme me rëndësinë që paraqet vota e 1.3 milion votuesve. Këto zhvillime kapërcejnë problematikën e ngritur më parë për këtë sistem.

Besimi në këtë sistem është sfida më e madhë në raport me koston apo kohën që nevojitet. Për këtë duhet një konsensus politik dhe shoqëror për realizimin e këtij votimi, duke u pasuar me ndërtimin e infrastrukturës institucionale dhe teknike.

Votimi përmes internetit ka avantazhet dhe dizavantazhet e tij, por nevojat specifike që ka shoqëria dhe shteti shqiptar për të mundësuar votën e gati gjysmës së votuesve duhet të mbizotërojnë kundrejt kundërshtive apo rreziqeve që paraqet aplikimi i këtij sistemi votimi, të ngritura në vendet e tjera, duke filluar nga SHBA.

Parregullsi zgjedhore apo shkelje ligjore kanë ndodhur në Shqipëri në

votimet klasike me fletë votimi në qendrat e votimit, nën mbikqyrjen fizike të administratës zgjedhore apo funksionarëve shtetërorë dhe agjencivë të zbatimit të ligjit. Suksesi në parandalimin dhe ndërshikimin e këtyre shkeljeve është çështje e sundimit të ligjit. Kjo nuk lidhet me llojin e votimit që aplikohet.

Për aplikimin e këtij sistemi do të duhej të ngrihej një strukturë e posaçme brenda administratës së lartë zgjedhore, me kompetenca, burime njerëzore dhe financiare të nevojshme për të realizuar këtë votim.

Me vendosjen e këtij votimi, do të jenë të nevojshme ndërhyrje legjislative në Kodin penal dhe Kodin e Procedurës Penale për parashikimin e veprave penale specifike dhe përfshirjen e këtyre veprave penale në kompetencën lëndore të Gjykatës kundër Korrupsionit dhe Krimit të Organizuar.

Për shkak të specifikës të këtyre krimeve zgjedhore, sidomos në rastet kur këto kryhen nga jashtë territorit të Shqipërisë është e nevojshme të vihen ne levizje mekanizmat e bashkëpunimit ndërshtetror mes organeve të zbatimit të ligjit dhe prokurorisë shqiptare me homologët e tyre në shtetet ku jetojnë shtetasit shqiptarë.

LITERATURA.

1. Kushtetuta e Republikës së Shqipërisë

2. Ligji nr. 10019/2008 “Kodi Zgjedhor i Republikës së Shqipërisë”, i ndryshuar.

3. Kodi Penal i Republikës së Shqipërisë, i ndryshuar.

4. Kodi i Procedurës Penale i Republikës së Shqipërisë, i ndryshuar.

5. Ligji nr.9034/2003 “Për emigrimin e shtetasve shqiptarë për motive punësimi”

6. Kodi i praktikes se mire ne çeshtjet zgjedhore udhezime dhe raporti shpjegues Miratuar nga Komisioni i Venecias në Mbledhjen e tij 52-të Plenare (Venecia, 18-19 Tetor 2002),

7. Udhëzues rreth nenit 3 të Protokollit nr. 1 të Konventës Evropiane të të Drejtave të Njeriut E drejta për zgjedhje të lira, Përditësuar më 30 prill 2017

https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_SQI.pdf

The International Institute for Democracy and Electoral Assistance - International IDEA) https://www.idea.int/data-tools/data/voter-turnout/compulsory-voting

Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member Stateson standards for e-voting

https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. https://rm.coe.int/168071bc84

Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. https://rm.coe.int/1680726c0b

European Parliament. Potential and challenges of e-voting in the European Union. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf

Electronic Voting Committee. General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia. Document: IVXV-ÜK-0.98 Date: 23 May 2016. https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf

Introducing Electronic Voting: Essential Considerations Policy Paper December 2011 fq.8. International IDEA Publications Office ISBN: 978-91-86565-21-3

Micha Germann. Internet voting increases expatriate voter turnout.

https://www.sciencedirect.com/science/article/abs/pii/S0740624X20303397?via%3Dihub

Drew Springall; Travis Finkenauer; Zakir Durumeric; Jason Kitcat; Harri Hursti; Margaret MacAlpine; J. Alex Halderman. Security Analysis of the Estonian Internet Voting System https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

Max Bader, Do new voting technologies prevent fraud? Evidence from Russia. USENIX Journal of Election Technology and Systems (JETS) Volume 2, Number 1 • December 2013 https://www.usenix.org/system/files/jets/issues/0201/jets_0201-bader.pdf

William J. Kelleher. Internet Voting in the USA: History and Prospects;.

https://www.eac.gov/sites/default/files/eac_assets/1/28/William-

Kelleher-Internet-Voting-WPSA-Paper-July-9th.pdf

8. Aviel Rubin. Professor of computer science at Johns Hopkins University and the technical director of the Johns Hopkins University Information Security Institute.

https://engineering.jhu.edu/magazine/2016/06/internet-voting-nonstarter/#.YrBLC3ZByMo

Minitri i Shtetit pwr Diasporwn. "Votimi i shtetasve të Republikës së Shqipërisë jashtë vendit" Informacion për Komisionin e Reformës Zgjedhore në Kuvendin e Shqipërisë' . https://diaspora.gov.al/wp-content/uploads/2018/07/VOTIMI-I-SHTETASVE-TE-REPUBLIKES-SE-SHQIPERISE-JASHTE-VENDIT.pdf

Banka e Shqipwrisw "Pandemia dhe Remitancat" https://online.fliphtml5.com/wpfxe/bbph/#p=4

Web të përdorura:

https://spectrum.ieee.org/online-voting-isnt-as-flawed-as-you-thinkjust-ask-estonia

https://www.swissinfo.ch/eng/electronic-voting_ten-arguments-for-and-against-e-voting/43959200

https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber-defences/

https://www.swissinfo.ch/eng/electronic-voting_ten-arguments-for-and-against-e-voting/43959200

https://www.openglobalrights.org/technology/

https://kqz.gov.al/results/results2021/results2021.htm

http://www.instat.gov.al/media/7848/diaspora-ne-shifra-2020.pdf

https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

Inter-Parliamentary Union http://archive.ipu.org/parline-e/reports/2001_arc.htm

KRIMI KIBERNETIK DHE SIGURIA KIBERNETIKE

EMILIANO LIKAJ

Abstrakt

Zhvillimi i vrullshësh i teknologjisë e ka transformuar menyrën tonë të jetesës, ku ndër të tjera ka bërë të mundur krijimin e një hapësire të re bashkëveprimi ndërmjet individëve në shoqëri, atë nëpërmjet internetit. Sot interneti është i aksesueshëm dhe mund të përdoret nga çdo individ pavarsisht moshës, nga kompani private dhe nga institucione shtetërore për një sër qëllimesh të ndryshme, si mbrojtja e vendit, marrja dhe shkëmbimi i informacionit, komunikimi, argëtimi, blerja e mallrave, shitja e mallrave etj.

Krahas gjithë lehtësirave dhe dobive që ky shërbim ofron, zhvillimi i teknologjisë së informacionit shoqërohet dhe me efekte anësore që kërcënojnë ndërveprimet sociale dhe ekonomike. Një nga problematikat kryesore është përdorimi i internetit në kundërshtim me qëllimin kryesor për të cilin ai është krijuar. Duke qënë se vlera dhe sasia e informacionit elektronik po rritet dita ditës, e ka kthyer atë në objektivin kryesor të sulmeve kibernetike të individëve keqdashës, grupeve të strukturuara kriminale dhe organizatave teroriste, padyshim të ndikuar dhe nga mundësia për të ruajtur anonimatin pas kryerjes së veprës penale.

Kjo situatë delikate dhe risitë që paraqiten në këtë fushë i ka vendosur institucionet shtetërore të zbatimit të ligjit dhe vet drejtësinë në një sprovë të re duke marrë në konsideratë faktit që krimet kibernetike kryhen lehtësisht në territorin e një apo disa shteteve njëkohësisht, pa prezencën fizike të personit apo personave që e kryejnë atë.

Në këtë punim do të trajtohen në mënyrë të detajuar por jo vetëm, krimet kibernetike kryesore, faktorët që ndikojnë në kryerjen e krimeve kiberenetike, dispozitat ligjore të vendit tonë dhe vendeve të tjera mbi krimet, konventat

ndërkombëtare të ratifikura nga Shqipëria, strategjitë lidhur me sigurinë kibernetike dhe problematikat kryesore që hasen gjatë bashkëpunimit ndërkombëtar në luftën kundër krimit kibernetik. Gjithashtu, nëpërmjet këtij studimi synohet të paraqiten rekomandime mbi masat që duhet të ndërmerren për përmirësimin e instrumenteve ligjor dhe strukturave të specializuara që përdoren në luftën kundër krimit kibernetik me qëllim parandalimin dhe reduktimin e tij, gjithashtu dhe forcimin e sigurisë kibernetike.

Fjalë kyçe: sulm kibernetik, krime kibernetike, siguria kibernetike, grupe të strukturuara kriminale, parashikime ligjore kombëtare dhe ndërkombëtare.

1. Hyrje

Referuar të dhënave në nivel botëror, mund të themi se hapësira kibernetike është sistemi më i madhë i ndërtuar ndonjëherë nga njeriu në nivel global. Edhe pse operimi në këtë hapsirë lidhet ngushtësisht me zhvillimin ekonomiko-social të shoqërisë, duke qënë se mund të aksesohet vetëm nëpërmjet pajisjeve elektronike të ndryshme si loaptop, kompjutera, tabletë, telefona inteligjentë etj., viti 2022 ka rregjistuar një përqindje rekord të përdoruesve të saj. Sipas Statistikave botërore të popullsisë dhe përdoruesve të internetit (World internete usage and population statistics) në vitin 2022, janë rregjistruar rreth 5,2 miliard përdorues të internetit osę rreth 66,2 % e popullsisë në nivel botëror[1].

Zhvillimi tekonologjik krijon produkte dhe shërbime të reja, duke lehtësuar kështu aktivitetin e shoqërisë në çdo fushe. Përdorimi i internet ka bërë të mundur kryerjen me efektivitet dhe shpejtësi të një sër shërbimesh në fushën të ndryshme si ajo ekonomike, mjekësore, juridike dhe në fusha të tjera. Mjafton një pajisje elektronike që një individ i caktuar të kryejë një veprim nga çdo vend i botës. Krahas anëve pozitive dhe lehtësirave të ndryshme që siguron, zhvillimi tekonoligjik ka dhe anët e veta negative pasi ka krijtuar një formë të re krimi, atë në fushën e kibernetikës. Vitet e fundit, kjo hapësirë ka shërbyer si burim për kryerjen e veprave të ndryshme penale si shpërndarja e materialeve pro gjenocidit ose krimeve kundër njerëzimit, kanosja me motive racizmi, pornografia, përgjimi i të dhënave kompjuterike, cënimi i privatësisë, mashtrimi kompjuterik, falsifikimi kompjuterik etj. Për shkak të kompleksitetit që paraqet identifikimi i autori të një apo disa veprave penale kibernetike e ka kthyer këtë hapsirën në një parajsë të veprimtarisë

1 https://www.internetworldstats.com/stats.htm pdf, fq 2

kriminale.

Duke parë përqindjen e lartë, fushat dhe qëllimet e ndryshme për të cilat shoqëria e përdor hapsirën kibernetike garantimi i sigurisë së saj është kthyer në shqëtësimin kryesore të shumë vende të botës. Për sigurinë kibernetike filloj të flitej rreth viteve 1970, kur studiuesi Bob Thomas krijoj një program të cilin e quajti Creeper. Ky program mund të lëvizte në rrjetin ARPNET duke lënë gjurmë kudo që shkonte. Për të luftuar këtë program, Ray Tomlison, shpikësi i e-mailit, krijoj programin Reaper[2], i cili ndoqi dhe shkatërroi programin Creeper. Reaper ishte shembulli i parë i antivirusit kompjuterik ose guri i parë në luftë kundër krimit konpjuterik.

Këshilli i Europës është një nga aktorët kryesor në luftën kundër krimit kompjuterik dhe ka dhënë një kontribut të rëndësishëm në garantimin e sigurisë kibernetike me anë të direktivave, vendimeve dhe rekomandimveve. Ashtu si shumë vende të tjera edhe Shqipëria po kalon tranzicionin e saj dixhital, ku një zhvillim i vrullshëm në fushën e teknologjisë është shënuar pas viteve 2000. Problematikat e sipërcituara dhe lufta kundër krimit kibernetik me qëllim garantimin e sigurisë kibernetike është gjithashtu në fokusin e vendin tonë, duke e detyruar atë të ndërmar hapa të rëndësishëm me qëllim përafrimin e legjislacionit të tij me atë të Bashkimit Europian dhe respektimin e parashikimeve ligjore në konventat ndërkombëtare të ratifikuara prej tij.

Pavarësisht se vendi ynë ka bërë disa hapa pozitiv në këtë aspekt, lufta kundër krimit kibernetik paraqet sfida të reja mjaft komplekse duke kërkuar domosdoshmërisht ndryshimin e dispozitave ligjore, forcimin e instrumenteve kombëtarë në luftën kundër krimit kibernetik dhe një bashkëpunim efikas ndërmjet shteteve.

2. Kuptimi dhe karakteristikat e krimit kiberneti

Duhet theksuar se për krimin kibernetik nuk ka një përkufizim të pranuar universalisht. Përgjithësisht, krimi kibernetik[3] kuptohet si një akt kriminalë ku kompjuterët dhe rrjetet janë shënjestër kryesore, përdoren si mjete për të kryer një vepër penale ose janë vendndodhja e krimit. Ndërsa me sulm kibernetik[4] kupohet çdo përpjekje e drejtuar/qëllimshme për të marrë akses,

2 https://cybermagazine.com/cyber-security/history-cybersecurity

3 Joseph, Aghatise E. (28 June 2006). "Cybercrime definition". www.crime-research.org.

4 https://csrc.nist.gov/glossary/term/Cyber_Attack

manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë dhe/ose disponibilitetin e të dhënave, të një aplikimi ose të të dhënave të sistemit kompjuterik, pa patur autoritet ligjor për ta bërë këtë.

Kompjuterat në krime kibernetike mund të shërbejnë si objekte, subjekte, dhe mjete:

- Janë objekte të krimeve kur ato sabotohen ose vidhen. Në shumë raste, kompjuterat janë goditur, djegur apo janë nxjerrë jashtë përdorimit me instrumente të caktuar. Dëmet, në këto raste, mund të jenë ndërkombëtare dhe të rënda, si psh dëmtimi i qëllimshëm i një infrastrukture financiare.
- Janë në rolin e subjekteve kur ato janë mjediset në të cilat zbatimet teknologjike kryejnë krime si psh., sulmet me viruse kompjuterike. Kur ndodhin krime kompjuterike, kompjuterat mund të jenë dhe subjekt i sulmeve.
- Roli i tretë i kompjuterave në krime është përdorimi i tyre si mjet për të prodhuar informacion të rremë apo që planifikojnë, kontrollojnë dhe luftojnë krime të cilat mund të kryhen në një të ardhme.

Përveç sa më sipër, aktorë të ndryshëm janë munduar t'i japin një përkufizim krimit kibernetik si për shembull:

- Sipas Departamentit Amerikan të Drejtësisë, me krim kompjuterik do të kuptojmë ato krime ku njohuria mbi sistemin kompjuterik është esenciale për kryerjen e një krimi të tillë;
- Sipas fjalorit të Oksfordit, njihen si krime kibernetike ato aktivitete kriminale të kryera me anë të kompjuterit ose internetit;
- Sipas Konventës së Budapestit, termi krim kompjuterik[5], është i ndarë në dy kategori :

  a) në një kuptim të ngushtë, me krim kompjuterik do të kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre;

  b) në një kuptim më të gjerë, me krim kompjuterik do të kuptohet çdo sjellje e paligjshme e kryer nëpërmjet një kompjuteri apo sistem kompjuterik, përfshirë krime të tilla si përpunimi i paligjëshëm i të dhënave kompjuterike, ofrimi apo shpërndarja

5 https://sq.wikipedia.org/wiki/Krimi_kompjuterik

> e informacionit nga një kompjuter apo rrjet, për të abuzuar dhe tërhequr vemëndjen me forma të tilla si ato për përkrahje të grupeve p.sh terroriste, neonaziste, pornografia dhe pedofilia. Këtu do të përfshihen edhe llojet e krimeve të mashtrimeve, duke shkelur sigurinë e rrjeteve si, bixhozi i paligjshëm, skemat piramidale, mashtrimi me karta krediti dhe lloje të tjera të aktiviteteve të paligjëshme. Në cyber crime, komponenti "cyber", zakonisht referohet për të kualifikuar shkeljet e reja të mundësuara nga teknologjia e informacionit apo ndërveprime të hapsirës kompjuterike, në shumë aktivitete tradicionale.

Krimit kibernetik është shumë i ndryshëm nga krimi tradicional. Dallimi kryesor ndërmjet tyre lidhet me faktin se krimi kibernetik përfshijnë çdo veprim kriminal që ka të bëjë me kompjuterin dhe rrjetin[6] ndërsa krimi tradicional shfaqet në forma të ndryshme.

Gjithashtu, këto dy sjellje kriminale dallojnë nga njëra-tjetra edhe sa i përket lënies së provave pas kryerjes së krimit. Në krimet tradicionale, autori i veprës penale gjatë kryerjes së saj lë prova të ndryshme si gjurmët e gishtave apo ndonjë provë tjetër fizike. Kjo gjë nuk ndodh në krimet kibernetike pasi prezenca fizike e autorit të vepës penale nuk është e nevojshme në vendin e kryerjes së krimit.

Një dallim tjetër i rëndësishëm lidhet me shfaqen e elementit të forcës. Në krimet tradicionale si vrasja, plagosja, rrëmbimi, vjedhja me dhunë, përdhunimi etj përfshihet ushtrimi i forcës e cila i shkakton dëmtime fizike viktimës. Nga ana tjetër në krimet kibernetike nuk kemi shfaqen e një elementi të tillë pasi përdorimi i forcës është i panevojshëm për kryerjen e një veprimi kriminal.

Për të kuptuar më mirë krimin kibernetik është e nevojshme analizimi i karakteristikave[7] kryesore të tij. Ndër to mund të përmendim:

- Kryhet nga njerëz me njohuri të specializuara. Duke qënë se këto vepra penale kryhen vetëm nëpërmjet teknologjisë, për kryerjen e një krimi të tillë autori duhet të jetë i arsimuar dhe të këtë njohuri të thelluara mbi përdorimin e kompjuterit dhe internetit.
- Mungesa e kufijve gjeografik. Krimi kompjuterik është një krim global, pasi në hapësirën kibernetike kufijtë gjeografikë nuk egzisotjnë. Me këtë ne kuptojmë që, një person mund të kryejë një vepër penale duke

6 https://www.webopedia.com/definitions/cyber-crime

7 https://lawpage.in/cyber_laws/crime/characteristics

qenë në një vend të caktuar në çdo kohë në çdo vend të botës. Pra, një haker i ulur në Kinë mund të hakojë një sistemin kompjuterik të vendosur në Francë.

- Kryhet në botën virtual. Veprimi i krimit kibernetik ndodh në hapësirën kibernetike dhe krimineli që po e kryen këtë vepër është fizikisht jashtë hapësirës kibernetike.
- Vështirësia në mbledhja e provave. Mbledhja e provave të një krimit kibernetik dhe paraqitja e tyre përpara gjyaktës është shumë e vështirë për shkak të natyrës së krimit kibernetik. Për kryerjen e një krimi kibernetik nuk është e nevojshme prezenca fizike e autorit në vendin e kryerjes së veprës penale.
- Madhësia e krimit është e paimagjinueshme. Krimi kibernetik ka potencialin për të shkaktuar lëndime dhe humbje jetësh në një masë që nuk mund të imagjinohet. Veprat penale si terrorizmi kibernetik, pornografia kibernetike etj. kanë shtrirje të gjerë dhe mund të shkatërrojnë faqet e internetit si dhe të vjedhin të dhënat e kompanive në një kohë të shkurtër.

3. Klasifikimi i krimeve kibernetike

Egzistojnë një sër ndarjesh dhe kategorizimesh të krimeve kibernetike. Kjo për shkak se disa prej studiuesve kanë marrë si element kryesor të klasfikimit të tyre se ndaj kujt është drejtuar një slum kibernetik, ndërsa disa të tjerë kanë martë si element bazë rolin e kumpjuterit në sulmin kibernetik[8]. Pavarsishtë shumëllojshmërive, e pranuar më gjerësisht është ajo ndarje që krimet kompjuterike i klasifikon në 4 kategori të mëdha:

1) Krim kibernetik ndaj individit (Akses/kontroll i pautorizuar i kompjuterit, shpërndarja e materialeve të turpshme, ngacmime dhe përndjekja kibernetike, shpifjet, spamming, e-mail spoofing);
2) Krim kibernetik ndaj pronës (vandalizmi kompjuterik, vjedhja e identitetit, krime ndaj pronës intelektuale, vjedhja e kohës së internetit);
3) Krim kibernetik ndaj qeverisë apo organizatve (terrorizmi kibernetik, kontroll i pautorizuar i kompjuterit, trojan horse, bombat logjike, sulmi Salami, kontaminimi i kompjuterit /infektimi me virus, mohimi i shërbimit, e-mail Bombing);

8 https://docplayer.net/61807742-Address-690-a-b-3-udoji-maratha-boarding-campus-gangapur-road-gangapur-road-nashik.html

4) Krim kibernetik ndaj shoqërisë (Falsifikimi, pedofilia dhe pornografia, web Jacking, terrorizmi kibernetik.

3.1 Krimet daj individëve[9]

Ngacmimet dhe përndjekja kibernetike[10]. Ngacimi dhe përndjekja bëhet duke ndjekur të gjitha lëvizjet dhe aktivitetit e një individi në internet. Përndjekja kompjuterike mund të realizohet në tre mënyra të ndryshme:

- Përndjekje me e-maile, ku autori i dërgon drejtpërdrejtë viktimës e-maile fyese ose ngacmuese,
- Përndjekja përmes internetit, në këto raste autori nuk sulmon hapsirën kibernetike të viktimës por publikon përmes internetit të dhëna personale të viktimës apo dhe foto të modifikuar në faqe pornografike apo faqe të ngjashme,
- Përndjekja përmes kompjuterit, ku autori synonë të marrë në dorë kompjuterin personal të viktimës.

Shpifjet[11]. Kjo ndodh kur shpifja bëhet me ndihmën e kompjuterave ose internetit. Për shembull kur dikush publikon materiale shpifëse për një person tjetër në një faqe interneti, ose dërgon e-maile që përmbajnë informacion shpifëse me qëllim dëmtimin e imazhit të viktimës.

Spamming[12]. Është ajo metodë që synon dërgimi i e-maile-ve në mënyrë masive me qëllimin mbledhjen e informacioneve , instalimin e një virusi apo kryerjen e një mashtrrim masivë. Mesazhe të tilla normalisht kanë një adresë fallco origjine me qëllim për të e zbuluar lehtësisht autorin e sulmit kibernetik.

E-mail spoofing[13]. Nëpërmjet kësaj metode autori i sulmit modifikon header-in e e-mail-it në mënyrë që e-maili të duket se e ka origjinën nga një burim i caktuar, por në të vërtetë është dërguar nga një burim i ndryshëm nga burimi i supozuar. Për shembull një haker mund të dërgojë një e-mail i cili duket sikur vjen nga PayPal, me mesazhin që llogaria juaj do të mbyllet nëse ju nuk klikoni linkun. Nëse përduresi i llogarisë mashtrohet nga ky e-mail

9 https://www.naavi.org/pati/pati_cybercrimes_dec03.htm

10 Avokati Parvez Mirza, https://astrealegal.com/internet-harassment-cyber-stalking-cyber-harassment-and-cyber

11 https://lawlex.org/lex-pedia/what-is-cyber-defamation/25167

12 https://cybercrime.org.za/spam

13 https://www.proofpoint.com/us/threat-reference/email-spoofing

dhe klikon linkun në fjalë, atëherë hakeri mund të vjedh paratë e viktimës.

Aksesi i paautorizuar në kompjuter. Një metode cila përdoret nga hakerat si ndaj individëve të ndryshëm ashtu dhe ndaj organizatave apo qeverive. Ky aktivitet quhet zakonisht hakerim, kur autori i veprës penale hyn në kompjuterin e viktimës pa dijenin e këtij të fundit.

3.2 Krime ndaj pronës

Vandalizmi kompjuterik[14]. Vandalizmi kompjuterik është një proces ku ekziston një program që kryen funksione jo normale dhe ka për qëllim nxjerrjen e fjalëkalimit të një përdoruesi ose të dhënave të tjera, apo fshirjen e hard diskut të kompjuterit të sulmuar.

Vjedhja e identitetit[15]. Hapësira kompjuterike përdoret për të marrë informacione personale të viktimave si numrin e kartës së kredit, patentën, fotografi etj., dhe duke i modifikuar, shtuar apo ndryshuar të dhënat e identitetit të personit, synon kryerje e veprimeve të ndryshme kriminale apo të marrë të drejta pasurore ose para, apo të përdorë kartat e kreditit apo llogarit bankare që i përkasin viktimës. Sipas studimit[16] të publikuar nga shoqëria Javelin stategy and Reasearch's, dëmi ekonomik i shkaktuar një veprimtari e tillë kriminale në vitin 2021, mendohet të kap shifrën e 52 bilion dollar. Rreth 42 milion qytetarë kanë qenë viktima të këtij sulmi.

Krime ndaj pronës intelektuale[17]. Qasja, shpërndarja dhe/ose përdorimi i pronësisë intelektuale pa dhe/ose përtej autorizimit fillestar dhe në shkelje të të drejtave të pronarit ose pronarëve të pronës intelektuale konsiderohet si krim i pronësisë intelektuale (a.k.a., vjedhja e pronës intelektuale). Këto krime përfshijnë kopjimin jo të ligjshëm të programeve, aplikacioneve, shpërndarja e tyre, shkeljen e të drejtave të autorit, shkeljen e markave tregtare etj, duke i shkaktuar në këtë mënyrë dëme të konsiderueshme financiare viktimës ose viktimave të veprës penale.

Vjedhja e kohës së internetit[18]. Nënkupton përdorimin e internetit nga personi i paautorizuar, kur në të vërtetë është paguar nga një person tjetër. Pra, nëpërmjet programeve të caktuara autori i veprës penale ndërhynë në

14 https://www.raiseupwa.com/users-questions/what-is-a-computer-vandalism

15 https://www.oaic.gov.au/privacy/data-breaches/identity-fraud

16 https://www.globenewswire.com/news-release/2022/03/29/2412099/0/en/Identity-Fraud-Losses-Total-52-Billion-in-2021-Impacting-42-Million-U-S-Adults.html

17 Module 11, Cybe- Enabled Intellectual Property Cime

18 https://www.ques10.com/p/49007/brief-explanation-of-cybercrime-classification-1

wireless-in e viktimës duke gjetur automatikisht pasuordin.

3.3 Krime ndaj qeverisë apo organizatave

Aksesi i paautorizuar në kompjuter[19]. Aksesi apo përdorimi i paautorizuar i kompjuterit pa dijenin e pronarit ose përdoruesit bëhet në dy mënyra:

a) Ndryshimi/fshirja e të dhënave,

b)Spiunazhi kompjuterik.

Spiunazhi kompjuterik ka të bëjë me zbulimin e "informacionit" apo "evidencave". Këto informacione merren për qëllime të ndryshme, të cilat mund të jenë për përfitime ekonomike, zublime të dhënash të rëndësishme të një kompani konkurente, marrjen e informacioneve sekrete etj. Në spiunazhin kompjuterik aktiviteti është gjithëmonë i panjohur dhe i paautorizuar.

Terrorizmi kibernetik[20]. Terrorizmi është ai lloj kërcënimi apo terrori kundër popullit apo qeverive i cili nuk parashikohet. Në këto raste autori i veprës penale shfrytëzon përdorimin e kompjuterit për të ngjallur terror tek të tjerët .Terrorizmi kompiuterik cilësohet si një çështje shumë sensitive. Përgjithësisht është përkufizuar si një sulm i paramenduar, politik, i motivuar kundër informacionit, sistemeve a programeve kompjuterike, dhe të dhënave të cilat pasojnë në dhunë, kundër shënjestrave nga grupeve ndërkombëtare. Si sulme terroriste mund të cilësohen dhe sulmet kompjuterike që synojnë dëmtimin e serverave qëndrorë të institucioneve shtetërore. Praktika botërore njeh raste të ndryshme të terrorizmit kibernetik si: sulmi kibernetik i lindjes së mesme i drejtuar kundër Izraelit në vitin 2000, ndëshkimi nga Kina në vitin 1999 ndaj institucioneve të SHBA-së, sulmi kibernetik nga grupi i quajtur Tamil Tigers në vitin 1998 në Sri Lankers apo dhe sulmi kibernetik i bërë ndaj NATO nga persona të kontraktuar nga Republika e Jugosllavisë.

E-mail Bombing[21]. Dërgimi i një numri të madh të e-maileve individëve, kompanive opo institucioneve shtetërore duke i nxjerrë e-mailet e tyre jashtë funksionit ose duke bërë që serverat e tyre të e-mailit të prishen. Gjithashtu nëpërmjet këtij sulmi mund të vendoset në dispozicion të përdoruesve të

19 https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

20 https://www.researchgate.net/profile/YarivTsfati/publication/233064294_WWWterrorismcom_Terror_on_the_internet/links/563fa6d208ae34e98c4e7340/WWWterrorismcom-Terror-on-the-internet.pdf; https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/9/09_chapter%201.pdf

21 https://www.ques10.com/p/49007/brief-explanation-of-cybercrime-classification-1

shumtë e-maili i viktimës.

Mohimi i shërbimit[22]. Dos (Denial of Service Atac – Mohim i Sherbimit) është ai sulm kompjuterik që drejtohet kundrejt një sistemi kompjuterik mëmë, i cili është përgjegjës për ofrimin e një shërbimi të caktuar. Autori i krimit kompjuterik shfrytëzon pikat e dobëta në sistemet operative ose në Protokollet e Internet si TCP/IP duke e ndërprerë shërbimin e sulmuar, dhe ndonjëherë të gjitha shërbimet e sistemit të shinjestruar mëmë. Me fjalë të tjera ky sulm u mohon përdoruesve të ligjshëm shërbimin e caktuar që ofron sistemi viktimë[23].

Lloje kryesore të këtij sulmi realizohen duke: Mbingarkuar zonën memorizuese të të dhënave që përpunohen; Sulmuar paketat shumë të vogla të informacionit; Dërguar mesazheve të keqinformuara apo të rreme; Ndërprerë komponentëve fizik të rrjetit; Dërguar një protokoll verifikues ICMP etj.

Kontaminimi i kompjuterit /infektimi me virus[24]. Një virus kompjuterik është një program i cili infekton programet e tjera që ndodhen në kompjuter . Viruset konsiderohen si një grup udhëzimesh kompjuterike të cilat synojnë të modifikojnë, shkatërojnë, regjistrojnnë, transmetojnë të dhëna ose programe të një kompjuteri, sistemi kompjuterash apo rrjeti kompjuterik. Gjithashtu ata uzurpojnë me sa është e mundur funksionim normal të kompjuterit.

Sulmi Salami[25]. Këto sulme përdoren për kryerjen e krimeve financiare. Është një seri sulmesh minore të cilat të marra së bashku përbëjnë një sulm të madh. Një slum i tillë synon të godasë sistemin bankar, pasi shuma të papërfillshme hiqen nga llogaritë e klientëve dhe grumbullohen derisa arrijnë një shifër të mëdha.

Bombat logjike[26]. Programe të tilla rrinë në pritje në kompjuterin e hakuar dhe bëhen efektive kur ndondh një verpim i caktuar në system. Në momentin që ndodh ngjarja e caktuar, i bëhet crash kompjuterit, duke lëshuar virusin. Kur një bombë logjike shpërthen, mund të jetë projektuar për të printuar një mesazh të rremë, për të fshirë ose korruptuar të dhëna kompjuterike apo të sjellë efekte të tjera të padëshirueshme nga viktima.

22 Po aty

23 https://docslib.org/doc/5313931/cyber-crime-practices-and-policies-for-its-prevention

24 CRIMES AND PUNISHMENTS, Chapter 205 Crimes Against Property NRS 205.4737 “Computer contaminant” define

25 Po aty

26 https://www.csoonline.com/article/2115905/logic-bomb.html

Trojan horse[27]. Është një program i paautorizuar i cili funksionon sikur të jetë një program i autorizuar, duke fshehur në këtë mënyrë atë që është në të vërtetë duke i bërë sistemit operativ.

3.4 Krime ndaj shoqërisë

Falsifikimi. Nëpërmjet kësaj vepre penale synohet të realizohet ndryshimi i të dhënave të regjistruara në një sistem kompjuterik. Në këtë rast, sistemi kompjuterik mund të jetë në shënjestër të aktivitetit krininal. Megjithatë, kompjuterat mund të përdoren edhe si mjete me të cilat kryhet falsifikimi.

Web Jacking. Hakerat krijojnë një faqe interneti të rreme, dhe kur kjo faqe hapet ajo të çon automatikisht në një faqe tjetër e cila dëmton sistemin kompjuterik të viktimës[28]. Më pas ata vihen në kontroll të faqes dhe mund të ndryshojnë përmbajtjen e faqes së internetit për përmbushjen e objektiviave politik , terroriste ose financiare.

Pedofilia dhe pornografia. Hapësira kibernetike është e aksesueshme nga të gjithë personat pavarsisht moshës. Gjithashtu ka një mungesë të theksuar të filtrimit të materiale që shfaqen në site të ndryshme gjë që i bën kryesisht fëmijët the adoleshentët te ekspozuar ndaj materiale pornografike. Ky fenomen cilësohet si një nga problematikat më aktuale dhe shqetësuese të shoqërisë.

Terrorizmi kibernetik. Është një sulm kompjuterik i cili drejtohet dhe shoqërisë përveç qeverive. Shpjegimin për këtë krim kompjuterit është bërë në seksioni e krimeve kompjuterike ndaj qeverisë apo organizatave.

Gjithastu këtu mund të listojmë dhe sjellje kriminale si bixhozi në internet, shitja e artikujve të paligjshëm, krime financiare etj.

4. Faktorët kryesor të kryerjes së krimeve kibernetike

Sipas ekspertëve studimi i anës psikologjise, kriminologjike dhe sociologjike të autorëve të krimeve kibernetike mund të sjellë pasoja pozitive në luftën kunder krimit kibernetik. Një rol të rëndësishëm luan gjithashtu dhe evidentimi i arsyeve kryesore që e motivojnë një haker për të kryer krime kibernetike, pasi përdoren si baza kryesore në hartimin e strategjive për garantimin e sigurisë kibernetike. Faktorët kryesorë të cilët çojnë persona të caktuar drejt kryerjes së krimeve kibernetike, qofshin këta objektiv apo subjektiv, janë të shumtë dhe nga më të ndryshimit, por më kryesorët po i

27 https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

28 https://www.cybercrimechambers.com/

rendisim më poshtë:

Për argëtim ose sfidë. Studiuesit besojnë se shumë kriminelë kibernetikë hakojnë jo për të bërë keq apo për përfitime financiare, por thjesht sepse munden. Ata mund të konsumojnë një vepër penale për të provuar aftësitë e tyre, ose mund ta shohin atë si një lojë. Sipas një raporti të vitit 2017 nga Agjencia Angleze Kombëtare e Krimit[29], 61 përqind e kriminelëve kibernetikë fillojnë aktivitetitn përpara moshës 16 vjeç. Studimi i Agjensisë Kombëtare të Krimit zbuloi gjithashtu se kurioziteti dhe dëshira për të rritur aftësitë ishin faktorët më të zakonshëm që çojnë në kryerjen e krimit kibernetik.

Për arsye financiare. Paratë janë arsyeja pas pothuajse të gjitha formave të krimit kibernetik, nga pirateria në internet e deri te mashtrimet dhe trafikimi i qënieve njerëzore. Sipas një studimi të kryer në prilli të vitit 2018 nga Dr. Mike McGuire, kriminelët kibernetikë mund të fitojnë më shumë se 166,000[30] dollarë në muaj.

Për arsye emocional. Shpesh herë kriminelët kibernetikë veprojnë të ndikuar nga emocionet personale, pavarësisht faktit nëse ata ndjejnë zemërim, hakmarrje, dashuri apo dëshpërim. Në këto raste autori i veprës penale mund të jetë një punonjës i pakënaqur ose i pushuar nga puna, dikush në konflikt me një të njohur, një person i cilët ka vuajtur bullizmin apo abuzimin në familje apo dikush i refuzuar. Përvoja ka treguar se shpesh herë motivet emocionale mund të jenë shkatëruese par viktimën e krimit kibernetik. Këto lloj veprash penale konsiderohen dhe si krime pasioni të kryera nëpërmjet internetit, duke qënë se në thelb të tyre qëndron pasioni i autorit të veprës penale.

Për motive ideologjike. Rreth 6% e krimeve kibernetike kryhen për arsye ideologjike ose morale[31]. Shembulli i njohur botërisht është seria e sulmeve që u krye nga "Anonymous" në serverat e kompanive financiare, kur këto të fundit nuk lejuan mbajtësit e llogarive dhe kartave të jepnin kontribute për WikiLeaks-in.

Për shkak të konkurrencës. Konkurenca është një faktor tjetër i rëndësishëm që shtyn persona të ndryshëm drejt krimeve kibernetike. Këto krime

29 Për më shumë https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file

30 Dr. Mike McGuire,"Into the Web of Profit" https://www.scribd.com/document/377159562/Into-the-Web-of-Profit-Bromium-Final-Report

31 https://cdn2.hubspot.net/hubfs/85462/2018/THIS%20WEEK/report_nuix_black_report_2018_web_us.pdf

zakonisht kryhen ndërmjet kompanive të mëdha me ndikim të rëndësishëm global, p.sh nga ose ndaj kompanive teknologjike, farmaceutikë,kompani që ofrojnë shërbime të përgjithshme etj.

Për motive politike. Për shkak të prezencës së internetit në shtëpinë e çdo individi, rëndom krimi kibernetik është përdorur si një mjet për të arritur qëllime politike. Shumë kompani, ku ndër më kryesoret mund të përmendim Facebook-un, përdorin informacione personale dhe të dhënat e përdoruesve të tij për të ndikuar në pikëpamjet politike të njerëzve. Ka pasur dhe raste kur krimi kibernetik është përdoret për të manipuluar zgjedhjet e një vendi.

5. Ligjet kibernetike në disa shtete të ndryshme

Shumica e shteteve sot në botë kanë miratuar ligje të shumta apo kanë nënshkruar konventa ndërkombëtare për të luftuar krimin kiberentik. Shtetet e Bashkuara të Amerikës kanë miratuar numrin më të madh të ligjeve specifike kibernetike, të ndjekura nga Mbretëria e Bashkuar, e cila fillimisht përveç ligjit kibernetik ka aplikuar në të njëjtën kohë dhe ligjet tradicionale për përballimin e disa rasteve shumë të vështira dhe komplekse[32]. Më poshtë do të sjellim disa nga ligjet kryesore të miratuar për të luftuar krimin kibernetik në disa shtete, ku normalisht do të fillojmë me dy shtetet e sipërpërmendura.

Shtetet e Bashkuara të Amerikës (SHBA) kanë një politikë shumë strikte për mbikëqyrjen elektronike dhe kanë miratuar ligje të ndryshme federale e shtetërore për mbrojtjen e kompjuterit dhe rrjetit kompjuterik nga krimet e ndryshme kibernetike. Ligji i parë i miratuar në këtë shtet, që i dha mundësin autoriteteve shtetërore për të ndjekur penalisht kriminelët kompjuterik, ishte Statuti i Mashtrimit me Tela (The Wire Fraud Statut)[33]. Ajo që duhet theksuar është se fillimisht ligjet kundër krimit kibernetik në këtë vend janë zhvilluar duke iu referuar shumicën e kohës ligjit të pronës. Në vitin 1986 kongresi miratoi Aktin për mashtrimin dhe abuzimin kompjuterik (Computer Fraud and Abuse Act "CFFA"), i cili teknikisht shikohej si një amendim i ligjit të vitit 1984, Akti Gjithëpërfshirës i Kontrollit të Krimit (Comprehensive Crime Control Act)[34].

Sipas ligjit një person është fajtor kur futet me vetëdije në një kompjuter

32 https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/9/09_chapter%201.pdf , fq 246

33 https://www.researchgate.net/publication/340756296_Law_Relating_to_Cyber_Crimes-_Comparative_Perspective

34 https://www.nacdl.org/Content/CFAABackground

apo program kompjuterik pa autorizim, ose pasi është futur në një kompjuter me autorizim, përdor mundësinë që aksesimi në kompjuter i ofron për qëllime të cilat nuk përfshihen në autorizim[35]. Ndërsa Akti i vitit 1986 parashikonte dënime shtesë për mashtrime dhe aktivitete të lidhura me pajisjet e aksesit dhe kompjuterët, si dhe mbrojtje shtesë për kompjuterët me interes federal. Ky akt shtoi gjithashtu tre ndalime të reja: neni 1030/a (4) që ndalon aksesin e paautorizuar me qëllim mashtrimi; seksioni 1030/a (5) që ndalon aksesin në një kompjuter pa autorizim dhe ndryshimin, dëmtimin ose shkatërrimin e informacionit; seksioni 1030/a (6) që ndalon trafikimin e fjalëkalimeve të kompjuterit[36].

Në vitin 1994 u miratua Akti për spiunazhin ekonomik[37], i cili synonte të mbronte sekretet tregtare nga sulmet kibernetike. Më pas, në vitin 1998 u miratua Akti për Mbrojtjen e të Dhënave, i cili u krijua për të mbrojtur të dhënat personale të ruajtura në kompjuter ose në rregjistra të organizuara në dosje[38]. Gjithashtu në SHBA, ekzistojnë dy ligje për pornografinë e fëmijëve të cilët kanë pësuar dhe disa ndryshime, Akti i Parandalimit të Pornografisë së Fëmijëve i vitit 1996 dhe Ligji për Mbrojtjen e Fëmijëve në internet i vitit 2000[39]. Ndërsa Akti i Mirësjelljes në Komunikim i vitit 1996 është miratuar për të mbrojtur të miturit nga pornografia.

Sa i përket aspektit procedurial në SHBA ekzistojnë rastet përjastimore kur realizimi i mbikqyrjes elektronike mund të realizohet pa urdhër gjykate. Kjo gjë u bë e mundur me anë të Aktit të Mbikëqyrjes së Inteligjencës së Huaj[40] (Foreign Intelligence Surveillance Act) të miratuar në vitin 1978, i cili pësoj ndryshime të mëvonshme[41]. Sipas këtij akti, Presidenti ka fuqinë për të autorizuar përgjime dhe mbikqyrje elektronike pa urdhër gjykate për mbrojtjen e vendit nga një sulm i mundshëm me pasoja të rënda, sabotazhi ose spiunazhi me kushtin që të mos përgjohen shtetas amerikanë[42]. Gjithashtu

35 https://www.nacdl.org/Content/CFAABackground

36 Po aty.

37 https://www.researchgate.net/publication/340756296_Law_Relating_to_Cyber_Crimes-_Comparative_Perspective

38 https://www.privacyhelper.co.uk/knowledge-hub-articles/data-protection-act-1998-a-summary-of-the-8-guiding-principles

39 https://www.ijrar.org/papers/IJRAR19D1056.pdf , fq 3

40 https://www.law.cornell.edu/uscode/text/50/chapter-36

41 Shumë parashikime të të cilave u panë si antikushtetuese, pasi u mundësua dhe përgjimi i shtetasve amerikanë pa urdhër gjykate, gjë e cila cënonte privatësinë. Kundër këtyre amendimeve te cilët mundësonin përgjim masiv pati shumë reagime. Kujto çështjen Edward Snowden, i cili demaskoi përgjimet masive të bëra nga SHBA.

42 https://www.law.cornell.edu/wex/electronic_surveillance

Presidenti ka autoritetin për të dhënë një mbikëqyrje të tillë, pa urdhër gjykate, nëpërmjet Prokurorit të Përgjithshëm për të marrë informacione të inteligjencës së huaj për një periudhë deri në 1 vit (USC 1802)[43].

Përveç sa më sipër, për të mos folur për aktet apo amendimet kundër terrorizmit dhe mbikqyrjen e mjeteve të komunikimit, në SHBA ka një numër të madh të ligjeve kibernetike të miratuara dhe të ndryshuara duke krijuar kështu një sistem ligjor të plotë për të trajtuar krimet e ndryshme në fushën kibernetike.

Lufta në Mretërinë e Bashkuar kundër krimit kibernetik ka kaluar në dy faza kryesore. Në fazën e parë ligjet tradicionale u aplikuan për të luftuar aktivitetin kriminal në internet. Ky realitet pasqyrohet në një sër rastesh të praktikës gjyqësore të kohës, ku mund të përmendim raste si Mbretëresha kundër Preddy dhe Mbretëresha kundër Gold dhe Schifreen[44]. Në një proces gjyqësorë të tillë ishte e vështirë për gjykatat dhe jurinë të zbatonin dispozitat e një akti i cili nuk ishte krijuar për situata të tilla, fakt i përforcuar dhe nga Lord Brendon[45] anëtar i Dhomës së Lordëve. Duke parë vështirësitë që hasi gjykata, u rrit së tepërmi presioni për hartimin dhe miratimin e një legjislacion specifik për krimin kompjuterik. Kjo çoi dhe në fillimin e fazës së dytë në luftën kundër krimit kompjuterik. Në këto kushte, bazuar në Raportin e Komisionit të ligjeve mbi "Keqpërdorimin e Kompjuterit" dhe disa rekomandimeve të tjera, në vitin 1990 u miratua Akti i Keqpërdorimit të Kompjuterit (Computer Misuse Act).

Ky akt përbën legjislacioni kryesor kundër krimit kibernetik në Mbretërinë e Bashkuar dhe trajton shumë nga sulmet kibernetike[46]. Sipas tij, "kompjuter" mund të nënkuptojë pajisje të tjera, të cilat ruajnë, përpunojnë ose marrin

43 https://www.ijrar.org/papers/IJRAR19D1056.pdf

44 https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/9/09_chapter%201.pdf fq 185

45 https://itlaw.fandom.com/wiki/R_v_Gold_%26_Schifreen#cite_note-1 Në përfundim të çështjes lordët lanë në fuqi vendimin e pafajsisë dhe Lord Brendon u shpreh: "*Rrjedhimisht, ne kemi arritur në përfundimin se gjuha e ligjit nuk kishte për qëllim të zbatohej për situatën që u tregua se ekzistonte në këtë rast. Depozitimi pas mbylljes së çështjes nga prokurorisë duhet të kishte pasur sukses. Është një përfundim që e arrijmë pa keqardhje. Përpjekja për t'i dënuar këto fakte në gjuhën e një Akti që nuk është krijuar për t'iu përshtatur atyre, prodhoi vështirësi të mëdha si për gjyqtarin ashtu edhe për jurinë, të cilat ne nuk do të dëshironim t'i shihnim të përsëriten. Sjellja e ankuesve ishte në thelb, siç u tha tashmë, sigurimi në mënyrë të pandershme e aksesit në të dhënave e bankës Prestel meanë të një mashtrim. Kjo nuk është vepër penale. Nëse mendohet se është e dëshirueshme të bëhet kështu, kjo është një çështje e legjislativit dhe jo e gjykatave*."

46 https://www.ramsac.com/blog/cybercrime-legislation-uk

informacion. Kjo do të thotë se legjislacioni për krimin kibernetik mbulon telefonat inteligjentë, tabletët dhe një mori pajisjesh të tjera teknologjike përtej kompjuterit tradicional desktop.

Ligji për Keqpërdorimin e Kompjuterit përcakton si të paligjshme dhe do të ndjekë penalisht[47]: Aksesin e paautorizuar, ose me qëllim të keq, në materialin e ruajtur në një kompjuter; Dëmtimin e qëllimshëm, duke përdorur sisteme kompjuterike; Modifikimin, heqjen ose shpërndarjen e të dhënave; Ndihmën në keqpërdorime kompjuterike, të tilla si ofrimi i informacionit.

Në Mbretërinë e Bashkuar, përpara miratimit të Ligjit për Keqpërdorimin e Kompjuterit, ekzistonin një sër ligjesh të tjera si: Ligji për çrregullimin e Industrisë së Telekomit (The legislation on deregulation of Telecon Industry), i vitit 1984, që synonte të mbronte interesat e konsumatorit dhe konkurencën e tregut[48]; E drejta e autorit (The Copyright), i vitit 1988, sjell një bazë ligjore të rëndësishme për të drejtën e autorit dhe ligjin e patentave[49]; Ligji i Vjedhjes dhe Ligji i Telekomunikacionit, që synonin të ndalonte keqpërdorimin e telekomunikacionit publik; Ligji për Përgjimin e Komunikimit (The Interception of Communication Act), që synonte të ndalonte falsifikimin dhe aktivitetet e tjera kriminale gjatë transmetimit nga sistemet publike të telekomunikacionit; Ligji për Mbrojtjen e të Dhënave (Data Protection Act),i vitit 1984, i cili synonte të mbronte të dhënat kompjuterike dhe bazën e të dhënave nga çdo shkelje ose dëmtim.

Pavarsisht miratimit të Ligjit për Keqpërdorimin e Kompjuterit, grafiku i aktiviteteve kriminale në internet në Mbretërinë e Bashkuar vazhdoi të rritej. Duhet thënë se Mbretëria e Bashkuar nuk ka një ligj gjithëpërfshirës të sigurisë kibernetike; në vend të kësaj, kuadri ligjor për sigurinë kibernetike është i shpërndarë në një sërë ligjesh të ndryshme: Fillimisht, Ligji për Mbrojtjen e të Dhënave (Data Protection Act) për të luftuar krimin kompjuterik dhe për të mbrojtur të dhënat kompjuterike u miratua në vitin 1998; Akti i Rregullores së Pushtetit Hetues i vitit 2000 (The Regulation of Investigatory Powers Act) i cil rregullon kompetenca hetimore të zbatimit të ligjit, të tilla si mbikëqyrja dhe përgjimi i të dhënave të komunikimit; Ligji për të ardhurat nga krimi (Proceeds of Crime Act) i vitit 2002, i cili synon fuqizimin e Policisë, Doganave dhe Gjykatave në lidhje me pastrimin e parave, kërkimin, sekuestrimin dhe konfiskimin e produkteve

47 https://www.legislation.gov.uk/ukpga/1990/18/contents

48 https://www.researchgate.net/publication/340756296_Law_Relating_to_Cyber_Crimes-_Comparative_Perspective

49 Po aty.

të krimit[50]; Ligji i Komunikimeve i vitit 2003 (The Communications Act) i cili zëvendësoi Aktin e Telekomunikacionit të vitit 1984. Ai konsolidoi rregullatorët e telekomunikacionit dhe transmetimit në Mbretërinë e Bashkuar, duke prezantuar Zyrën e Komunikimeve si rregullatorin e ri të industrisë[51]. Gjithashtu përfshin garantimin e sigurisë kibernetike që zbatohen në sektorin e telekomunikacionit nga ofruesit e rrjeteve publike të komunikimeve elektronike dhe ofruesit e shërbimeve publike të komunikimeve elektronike; Rregulloret e Privatësisë dhe Komunikimeve Elektronike[52] (The Privacy and Electronic Communications Regulations) e vitit 2003, e cila synon të garantojë për individët të drejta specifike të privatësisë në lidhje me komunikimet elektronike; Ligji për mashtrimin (The Fraud Act) i vitit 2006, e përkufizoi mashtrimin si një vepër penale e cila mund të kryhet nga përfaqësimi i rremë, nga moszbulimi i informacionit ose nga shpërdorimi i pozitës[53]. Qëllimi është elementi më i rëndësishëm i kësaj vepre penale sipas këtij ligji; Akti i Rregullores së Pushtetit Hetues i vitit 2016 (The Regulation of Investigatory Powers Act) ndryshon ligjin e vitit 2000 duke parashikuar kompetenca shtesë hetimore dhe krijuar veprën penale të përgjimit të paligjshëm të komunikimeve[54]; U miratua Akti i Mbrojtjes së të Dhënave në vitin 2018, i cili kontrollon se si përdoren informacionet personale të individëve nga organizata, biznese apo dhe nga qeveria[55]; Rregulloret e Rrjetit dhe Sistemeve të Informacionit e vitit 2018 (The Network and Information Systems Regulations) ofrojnë masa ligjore për të rritur nivelin e sigurisë (si në kibernetike ashtu edhe elasticitetin fizik) të rrjeteve dhe sistemeve të informacionit për ofrimin e shërbimeve thelbësore dhe shërbimeve dixhitale[56].

Pavarsisht problematikave të shumta që hasen në praktik dhe numrit gjithmonë në rritje të krimeve kompjuterike, Mbretëria e Bashkuar ka një legjislacion mjaft të pasur për të luftuar krimin kibernetik.

Parlamenti i Indisë ka miratuar ligjin e parë për të luftuar krimin kibernetik në vitin 2000, të quajtur Ligji i Teknologjisë së Informacionit (Infomation Technology Act)[57]. Ky ligj do të sillte ndyshime në Kodin Penal

50 http://www.oas.org/juridico/PDFs/mesicic5_bhs_proceedsact_annex38.pdf
51 https://en.wikipedia.org/wiki/Communications_Act_2003
52 https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr
53 https://trustpair.fr/en/blog/the-fraud-act-2006-and-what-it-means-for-companies
54 https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
55 https://www.gov.uk/data-protection
56 https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
57 https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Indian (Indian Penal Code) të vitit 1860, në Ligjin e Provave Indiane (Indian Evidence Act) të vitit 1872, Ligjin e Evidentimit të Librave të Bankierëve (Bankers Books Evidence Act) të viti 1891 dhe Ligjin e Bankës së Rezervës të Indisë (Reserve Bank of India) të vitit 1934[58]. Miratimi i këtij ligji bëri të mundur trajtim e veprave penale që kryhen në formë elektronike ose që kanë të bëjnë me kompjuterin, sistemin kompjuterik dhe rrjetet kompjuterike, por gjithashtu solli me vete vështirësi të reja pasi avokatët, oficerët e policisë, prokurorët dhe gjyqtarët shpesh nuk kuptonin terminologjin shumë teknike të përdorur në këtë akt. Gjithashtu ky ligj paraqiste mangësi sa i përket parashikimeve mbi shumë krime kibernetike. Për të garantuar luftimin e krimit kibernetik u pa e domosdoshme ndryshimi dhe amendimi i këtij ligji, i cili erdhi në vitin 2008 nëpërmjet Amendimit të Ligjit të Teknologjisë së Informacionit.

Ky amendim shtoi: seksionin 66 A i cili trajtonte dërgimin e mesazeve fyese nëpërmjet shërbimit të komunikimit, seksionin 66 B i cili trajtonte marrjen e pandershme të burimeve të vjedhura nga kompjutera apo pajisje komunikimi, seksionin 66 C i cili parashikonte dënim për vjedhjen e identitetit, seksionin 66 D i cili trajtonte mashtrimin me identitetin duke përdorur burimet kompjuterike, seksionin 66 E i cili trajtonte cenimin e privatësisë, seksionin 67A, B C i cili parashikon ndëshkim për publikimin dhe transmetimin e materialeve pornografike. Gjithashtu solli parashikimin e veprave penale si aksesimi në një sistem kompjuterik të mbrojtur, thyerja e konfidencionalitetit dhe privatësisë, terrorizmi kibernetik, sulmet kompjuterike ndaj kompanive, sulmet ndaj firmave elektronike të certifikuara si dhe i dha kompetencën çdo oficeri që nuk është poshtë rankut të inspektorit të hetojë çdo krim kibernetik sipas këtij amendimi[59]. Sa i përket luftës ndaj krimit kibernetik në Indi, një rol të rëndësishëm dhe ndihmues ka luajtur dhe gjykata nëpërmjet vendimeve të saj.

Çdo shtet në Australi është i pavarur dhe ka territorin e vet, parlamentin, gjyqësorin dhe ekzekutivin e vet, pavarsisht se ligjet federale prevalojnë ndaj atyre të secilit shtetet. Duke qënë se krimi kibernetik është pa kufij, në Australi është Commomnwealth që ka miratuar regjimin legjislativ për të luftuar atë. Për këtë arsye shtetet që përbëjnë Australin kanë një rregjim juridik të brendshëm të varfër sa i përket krimit kibernetik. Për shembull shteti i Queensland ka vetëm dy dispozita në Kodin Penal[60] të cila lidhen me

58 https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/9/09_chapter%201.pdf , fq 98

59 Lexo po aty, fq 96-145

60 https://www.legislation.qld.gov.au/view/pdf/inforce/current/act-1899-009

internetin dhe kompjuterin, të cilat prekin: përdorimin e internetit, mbrojtjen e fëmijëve nën 16 vjeç dhe hakimin e keqpërdorimin kompjuterik.

Ligji kryesor për luftimin e krimit kibernetik në Australi është Ligji i Kirmit Kibernetik (Cybercrime Act)[61] i cili u miratua në vitin 2001, por nga ai moment është amenduar herë pas here. Përpara se të vendosej ligji i sipërpërmendur, dispozitat ligjore të Commonwealth për krimin kompjuterik gjendeshin në Ligjin e krimeve (Crime Act) të vitit 1914, Ligjin e Privatësisë[62] të vitit 1988 (Privacy Act), ligjin e Telekomunikacionit (Telecommunications Interceptions and Access) i vitit si 1979 dhe në Kodin Penal (Commonwealth Criminal Code) të 1995[63].

Ligji i Krimit Kibernetik, bazuar në modelin e Ligjit të Keqpërdorimit të Kompjuterit të miratuar në Angli, solli në legjislacionit e vendit parashikime të detajuara mbi sulmet ndaj kompjuterit. Në këtë ligj u bënë dhe përkufizime të koncepteve si ai të dhënave dixhitale, komunikimit elektronik dhe shërbimeve të telekomunikacionit.

Qeveria e Australisë në gusht të vitit 2012 miratoi Amendimin e Ligjit të Krimit Kiberentik (Cybercrime Legislation Amendment Act), qëllimi i të cilit ishte të bënte të mundur implementimin e Konventë së Këshillit të Europës për Krimin Kibernetik. Ky ligj ndryshoi katër pjesë të legjislacionit[64]: Aktin e Telekomunikacionit të vitit 1997, Aktin e Telekomunikacionit mbi Aksesin dhe Ndërhyrjen1979, Ligji për Ndihmën e Ndërsjellë në Çështjet Penale 1987 dhe Ligji i Kodit Penal 1995.

Ndryshimet në legjislacion lidheshin me regjimin e ruajtjes së komunikimeve të arkivuara, ndihmën e ndërsjellë, amendimin e shkeljeve kompjuterike dhe konfidencialitetin e të dhënave të telekomunikacionit. Megjithëse shumica e ndryshimeve u bënë në vitin 2012, ato hynë në fuqi në Kodin Penal vetëm më 1 mars 2013.

Së fundmi, në vitin 2018 Qeveria Australiane miratoi dhe Ligjin e Sigurisë së Infrastruktureës Kritike (The Security of Critical Infrastructure Act)[65]. Nëpërmjet tij synohej të menaxhoheshin risqet e sigurisë kombëtare nga sabotazhi, spiunazhi dhe detyrimet e paraqitura nga subjektet e huaja[66]. U

61 https://rm.coe.int/cybercrime-act-2001/16808e70b4

62 https://www.legislation.gov.au/Series/C2004A03712

63 https://www.legislation.gov.au/Details/C2021C00183

64 https://lr.law.qut.edu.au/article/download/541/545/541-1-1305-2-10-20151118.pdf

65 https://www.legislation.gov.au/Details/C2018A00029

66 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018

vendosën detyrimime mbi subjekte që ushtronin aktivitetin e tyre në sektorë si ai i energjisë elektrike, komunikimeve, ruajtjes ose përpunimit të të dhënave, shërbimeve financiare dhe tregjeve, ujit, kujdesit shëndetësor dhe mjekësor, arsimit të lartë dhe kërkimit, ushqimit, transportit, teknologjisë hapësinore dhe industrisë së mbrojtjes[67]. Ky ligj pësoi ndryshime të tjera të rëndësishmë në dhjetor të vitit 2021 dhe në mars të vitit 2022 duke shtuar kështu rregullat si dhe sektorët në të cilën do të aplikoheshin këto rregulla.

Ka dhe shumë shtete të tjera në botë ku studimi i luftës së krimit kibernetik është kompleks dhe mjaft interesant. Një ndër këto është dhe Kina ku censura e internetit është ekstreme për shkak të numrit të lartë të ligjeve dhe rregulloreve administrative. Më shumë se gjashtëdhjetë rregullore për internetin janë krijuar nga qeveria e Kinës, e cila ka dhe sistemin e kontrollit të internetit më të gjerë dhe më të avancuar se në çdo vend tjetër në botë. Autoritetet qeveritare jo vetëm që bllokojnë përmbajtjen e faqeve të internetit, por gjithashtu monitorojnë aksesin e individëve në internet. Që nga maji 2015, Wikipedia kineze është bllokuar në Kinë. Kjo u bë pasi Wikipedia filloi të përdorte kriptim HTTPS, i cili e bëri të pamundur ose më të vështirë censurën selektive.

6. Instrumentet ndërkombëtarë të ratifikuara nga Shqipëria lidhur me krimin kibernetik dhe legjislacioni i brendshëm

Dispozitat e para penale në fushën e krimit kompjuterik në vendin tonë jan sanksionuar në datën 24.01.2001 me anë të ligjit nr. 8733, "Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.01.1995, Kodi Penal i Republikës së Shqipërisë". Nëpërmjet këtij ligji u parashikua si vepër penale "Ndërhyrja në transmetimet kompjuterike" në nenin 192/b[68] dhe "Përdorimi i paligjshëm i teknologjisë së lartë" në nenin 286/a[69] të Kodit Penal. Megjithatë këto

67 https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure

68 Neni 192/b, Kodi Penal pas ndryshimit të bërë nëpërmjet Ligjit nr. 873, datë 24.01.2001 – **Ndërhyrja në tansmetimet kompjuterike.** "*Ndërhyrja në çdo formë, në transmetimet dhe programet kompjuterike, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në tre vjet.Po kjo vepër, kur ka sjellë pasoja të rënda, dënohet me burgim gjer në shtatë vjet.*" Dispozi e cila pësoi ndryshime me ana të ligjit nr. 10023, datë 27.11.2008 për të qënë në harmoni me Konventën e Budapestit.

69 Neni 286/a, Kodi Penal pas ndryshimit të bërë nëpërmjet Ligjit nr. 873, datë 24.01.2001- **Përdorimi i paligjshëm i teknologjisë së lartë.** "*Prodhimi dhe përdorimi i sistemeve telematike, mjeteve dhe pajisjeve të teknologjisë së lartë, në rastet e veprave penale të parashikuara në nenet 283 gjer 286/a të këtij Kodi ose për të mundësuar ose lehtësuar konsumimin e lëndëve narkotike dhe psikotrope ose për të transmetuar a përhapur njoftime publicitare për stimulimin e përdorimit të tyre, dënohet me burgim gjer në*

dispozita do të konsideroheshin nga ekspertët e studimit të ligjit si dispozita me karakter të përgjithshëm dhe sintetik, përmbajtja e të cilave nuk mjaftonte për të mbuluar veprimtaritë e ndryshme në fushën kibernetike.

Pas 1 viti, me anë të ligjit nr. 8888 datë 25.04.2002, Shqipëria ratifikoi "Konventën për Krimin Kibernetik" e miratuar nga Komiteti i Ministrave të Këshillit të Europës dhe u hap për nënshkrim në Budapest, më 23 Nëntor 2001, në Konferencën Ndërkombëtare për Krimin Kibernetik. Kjo konventë shihet si instumenti më i rëndësishëm europiane në luftën kundër krimit kibernetik. Dy vite më vonë vendi ynë ratifikoi dhe Protokollin shtesë të kësaj Konvente "Per penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nepërmjet sistemit kompjuterik"[70]. Në këtë mënyrë vendi ynë e bëri këtë instrument pjesë të sistemit të brendshëm juridik, bazuar në nenit 122 të Kushtetutës së Shqipërisë[71], dhe mori përsipër detyrimin për të reflektuar parashikimet e kësaj Konvente në legjislacionin e tij të brendshëm.

Edhe pse Konventa u ratifikua në vitin 2002 dhe hyri në fuqi në vitin 2004, implementimi i saj në Kodin Penal dhe Kodin e Procedurës Penale u bë vetëm në vitin 2008 me ana të ligjit nr. 10023, datë 27.11.2008 dhe ligjit nr.10054, datë 29.12.2008, nëpërmjet të cilëve u reflektuan dhe parashikimit e protokollit shtesë.

Duhet pranuar se Shqipëria vitet e fundit ka ndërmarr një sër hapash pozitiv sa i përket vendosjes dhe implementimit të standarteve ndërkombëtarë në luftën ndaj krimit kibernetik , gjë e cila rrjedhimisht sjellë përmirësimin e sistemit kombëtar ligjor të vendit tonë. Përmirësim pati dhe ligji procedurial, ku në vitin 2008 u bënë ndryshime të rëndësishme në Kodin e Procedurës Penale të Republikës së Shqipërisë sa i perket mjeteve të kërkimit të provave në rastet e veprave penale kompjuterike. Gjithashtu në vitin 2017 ligji procedurial penal pati ndryshime lidhur me veprimet hetimore mbi provat kompjuterike.

Nga studimi i Kodit Penal vemë re se veprat penale kompjuterike të

pesë vjet." Dispozi e cila pësoi ndryshime me ana të ligjit nr. 10023, datë 27.11.2008 për të qënë në harmoni me Konventën e Budapestit.

70 https://www.pp.gov.al/rc/doc/protokolli_shtese_i_konventes_per_krimin_kibernetik_1371.pdf

71 Nenin 122 pika 1 e Kushtetutës parashikon:
"*Çdo marrëveshje ndërkombëtare e ratifikuar përbën pjesë të sistemit të brendshëm juridik pasi botohet në Fletoren Zyrtare të Republikës së Shqipërisë. Ajo zbatohet në mënyrë të drejtpërdrejtë, përveç rasteve kur nuk është e vetëzbatueshme dhe zbatimi i saj kërkon nxjerrjen e një ligji. Ndryshimi, plotësimi dhe shfuqizimi i ligjeve të miratuara me shumicën e të gjithë anëtarëve të Kuvendit për efekt të ratifikimit të marrëveshjeve ndërkombëtare bëhet me të njëjtën shumicë*".

implementar në vitin 2008 nuk jank të vendosura në një kre të veaçntë të Kodit Penal, por janë të shpërndara në krerë të ndryshëm në varësi të objektit juridik që ato mbrojnë. Të njëjtën mënyrë sanksionimi ka dhe shumica e vendeve anëtarë të Bashkimit Europian apo dhe e vendeve të cilët kanë ratifikuar këtë konvent. Në ndryshim nga legjislacionet e brendshme të vendve të ndryshme, Konventa për Krimin Kibernetik[72] i ka vendos krimet kibernetike, duke marrë në konsideratë formën e shfaqes së tyre, duke i ndarë në veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike, krimet e lidhura me kompjuterët, vepra penale të lidhura me përmbajtjen dhe vepra penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura me të.

Legjislatori ka krijtar tashmë bindjen se veprat penale në fushën kompjuterike kanë një natyrë të veaçantë dhe pasoja e tyre mund të vijë në një vend të ndryshëm nga ai i kryerjes së veprimit kriminal. Në funksion të kësaj logjike, legjislatori ka shtuar në Pjesën e Përgjithshme të Kodit Penal dhe më konkretisht në nenin 7 të tij, shkronjën "j"[73], duke përmbushur kështu dhe detyrimin ligjor që rrjedh nga artikulli 22 i konventës së Budapestit.

Përveç ndryshimit të sipërcituar, Ligji nr. 10023/2008 ka sjellë një sër ndryshimesh të tjera në pjesën e Posaçme të Kodit Penal[74], ku u shtuan vepra penale si: Në nenin 74/a u shtua verpra penale "Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit¨; Në nenin 84/a u shtua vepra penale ¨Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik"; Në nenin 119/a u shtua verpra penale "Shpërndarja e materialeve raciste ose ksenofobie nëpërmjet sistemit kompjuterik"; Në nenin 119/b u shtua verpra penale "Fyerje me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik"; Në nenin 143/b u shtua verpra penale "Mashtrimi kompjuterik"; Në nenin 186/a u shtua verpra penale "Falsifikimi kompjuterik"; Në nenin 192/b u shtua verpra penale "Hyrja e paautorizuar kompjuterike"; Në nenin 293/a u shtua verpra penale "Përgjimi i paligjshëm i të dhënave kompjuterike"; Në nenin 293/b u shtua verpra penale "Ndërhyrja në të dhënat komjuterike"; Në nenin 293/c u shtua verpra penale "Ndërhyrja në sistemet kompjuterike"; Në nenin 293/ç u shtua verpra penale "Keqpërdorimi i pajisjeve"; Në nenin 293/d u shtua verpra penale "Shitja e pa autorizuar e kartave SIM".

72 https://rm.coe.int/1680081561 "Konventën për Krimin Kibernetik".

73 Në këtë pikë përcaktohet se "Ligji penal i Republikës së Shqipërisë është i zbatueshëm edhe për shtetasin e huaj që jashtë territorit të Republikës së Shqipërisë, kryejnë vepra penale në fushën e teknologjisë së informacionit, në dëm të interesave të shtetit ose të shtetasve shqiptar".

74 Shiko ligjin nr. 10023, datë 27.11.2008 "*Për disa shtesa dhe ndryshime në ligjin nr. 7859, datë 27.01.1995, Kodi Penal i Republikës së Shqipërisë, i ndryshuar*"

Ndërsa në Kodin e Procedurës Penale[75] u shtuan parashikimet si më poshtë: Në nenin 191/a, "Detyrimi për paraqitjen e të dhënave kompjuterike"; Në neni 208/a, "Sekuestrimi i të dhënave kompjuterike"; Në nenin 299/a, "Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike"; Në nenin 299/b, "Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike".

Përveç sa më sipër, legjislatori i vendit tonë ka hartuar e miratuar dhe disa ligje të tjera të rëndësishme që lidhen me sigurinë dhe krimin kibernetik si: Ligji nr. 2/2017, "Për sigurinë kibernetike"; Ligji nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar; Ligji nr. 9887, datë 10.3.2008, "Për mbrojtjen e të dhënave personale", i ndryshuar; Ligji nr. 8457, datë 11.2.1999, "Për informacionin e klasifikuar", i ndryshuar; Ligji nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", i ndryshuar; Ligji nr. 107, datë 15.10.2015, "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar etj.

Ashtu si në vendet e tjera edhe në vendin tona janë krijuar një sër institucionesh përgjegjëse për të garantuar sigurinë kibernetike ku ndër më të rëndësishmit përmendim: Policinë e Shtetit e cila është përgjëgjësë për parndalimin dhe hetimin e krimit kibernetik[76], Prokurorinë e Përgjithshme e cila ushtron ndjekjen penale në fushën e kibernetikës[77], Agjencinë Kombëtare për Sigurinë Kompjuterike e ngarkuar me detyrën për mbrojtje ndaj sulmeve kibernetike[78], Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike i ngarkuar me detyrën për të garantuar zbatimin e ligjit Nr. 8457/2008[79], Autoritetin e Komunikimeve Elektronike dhe Postare i ngarkuar me detyrën për të mbrojtur të dhënat personale[80], Agjencinë Kombëtare të Shoqërisë së Informacionit e cila garanton siguri për aktivitetin e administratës publike[81], Drejtorinë e Sigurimit të Informacionit të Klasifikuar e cila garanton sigurinë e sistemeve të klasifikuara[82], Drejtorinë

75 Shiko ligjin nr.10054, datë 29.12.2008, "*Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 17.03.1995, Kodi i Procedurës Penal i Republikës së Shqipërisë, i ndryshuar*"

76 Për më shumë https://mb.gov.al/wp-content/uploads/2018/02/LIGJI_I_POLICISE_SE_SHTETIT_-_2014.pdf

77 https://www.parlament.al/Files/Akte/20210331134914ligj%20nr.%2042,%20dt.%2023.3.2021.pdf

78 VKM nr. 776, datë 14.09.2011 "Për krijimin e Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT)"

79 https://cesk.gov.al/legjislacioni/index.html

80 https://akep.al/en

81 https://akshi.gov.al/akshi

82 https://www.nsa.gov.al

e Shifrës përgjegjëse për sigurinë e komunikimit[83], Shërbimin Informativ të Shtetit i cili ka për detyrë zbulimin e sulmeve që kërcënojnë sigurinë e vendit[84] etj.

7. Analizë juridiko-penale e disa prej veprave penale kompjuterike

Për shkak të rëndësisë, impaktik dhe përhapjes së veprave të sipërcituara në vendin tonë më poshtë do të paraqes një analizë juridiko-penale të detajuar mbi veprat penale të mashtrimit, falsifikimit kompjuterik dhe hyrjes së paautorizuar kompjuterike.

Vepra penale e ¨Mashtrimit kompjuterik¨ është e sanksionuar në nenin 143/b[85] të Kodit Penal të Republikës së Shqipërisë.

Kjo dispozitë është vendosur në Kreun III të Pjesës së Posaçme të Kodit Penal, ku parashikohen veprat penale kundër pasurisë dhe në sferën ekonomike. Për rrjedhojë, objekti i kësaj dispozite është mbrojtja e marrëdhnieve juridike të vendosura për të garantuar të drejtën e pronës private dhe publike nga veprimet apo mosveprimet e kundraligjshme.

Nga ana objektive kjo vepër penale kryhet nëpërmje futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike dhe duke ndërhyrë në funksionimin e një sistemi kompjuterik. Pavarsisht se ana objektive e kësaj vepre penale përshkruhet në dispozitë, ajo çka paraqet vështirës është kuptimi i qartë i veprimeve të sipërpërmendura, çka ndihmon për të përcaktuar nëse ndodhemi përpara konsumimit të anës objektive të kësaj vepre apo jo. Shpjegimi i këtyre veprime mund të bëhet në mënyrë të saktë vetëm duke ju referuar relacionin shpjegues të Konventës për Krimin Kibernetik.

Subjekti i kësaj veprë penale mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm sipas ligjit.

---

83 https://akep.al/wp-content/uploads/2021/07/LIGJI-NR.-8457-Per-Informacionin-e-Klasifikuar-1-1.pdf

84 https://www.shish.gov.al/

85 Neni 143/b i Kodit Penal – **Mashtrimi kompjuterik**, "*Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.*
Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet".

Nga ana subjektive kjo vepër penale kryhet me dashje të drejtpërdrejtë, pasi autori ka pas qëllim nxjerrjen e përfitimeve materiale për vete ose persona të tjerë duke marrë pasurinë e një personi tjetër qoftë ky fizik, juridik apo shtetërore. Pra mendimi kriminal zhvillohet brenda autorit të veprës penale përpara se ky i fundit të ndërmarrë veprime për kryerjen e veprës penale.

Gjithashtu në paragrafin e dytë të kësaj dispozite parashikohen dhe rrethanat cilësuese të kësaj vepre penale. Konsiderohen rrethana cilësuese: kur vepra penale është kryer në bashkëpunim, pra nga dy ose më shumë persona; kur vepra penale është kryer ndaj dy ose më shumë personave; kur vepra penale është kryer më shumë se një herë, pra kur mashtrohen disa herë persona të ndryshëm ose i njëjti person brenda një interval kohor, me kushtin që autori i veprës penale të mos jetë dënuar me vendim të formës së prerë per krimin e parë; kur vepra penale ka sjellë pasoja të rënda kriminale.

Një tjetër vepër penale është Falsifikimi Kompjuterik i sanksionuar në nenin 186/a[86] të Kodit Penal të Republikës së Shqipërisë. Kjo dispozitë është vendosur në Kreun VIII të Pjesës së Posaçme të Kodit Penal, ku parashikohen vepra penale për falsifikimin e dokumentave dhe është hartuar në përputhje me atë që kërkohet nga Konventa e Budapestit. Sanksionimi i një dispozite të tillë u bë tejet i rëndësishëm duke parë se tashmë veprimtaria e apratit shtetëror dhe gjenerimi i dokumenteve të ndryshme bëhet në mënyrë elektronike.

Objekti i veprës penale janë marrëdhëniet juridike të vendosura për mbrojtjen e interesave publik nga sulmet e ndryshme kompjuterike.

Nga ana objektive krimi kryhet nëpërmjet futjes, ndryshimit, fshirjes, heqjes pa të drejtë të të dhënave kompjuterike, për të siguruar e më pas për të përdorur dokumentat e reme.

Subjekti mund të jetë i përgjithshëm ose i posaçëm. Sipas paragrafit 1 të kësaj dispozite subjekt mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm. Referuar pargrafit të dytë subjekti është gjithëmonë i posaçëm pasi është i ngarkuar me detyrëm par të ruajtur të dhënat kompjuterike.

---

86 Neni 186/a i Kodit Penal – **Falsifikimi Kompjuterik,** *"Futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.*
Kur kjo vepër kryhet nga personi, që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike, në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda për interesin publik, dënohet me burgim tre deri në dhjetë vjet".

Nga ana subjektive vepra penale kryhet me dashje të drejtpërdrejtë dhe ka qëllim përdorimin e të dhënave të reme të siguruara si autentike.

Në paragrafin e dytë të kësaj dispozite parashikohet si rrethanë cilësuese rastet kur: kjo vepër penale kryhet nga personi i cili ka për detyrë ruajtjen dhe administrimin e të dhënave kopjuterike, pra subjekti i veprës penale në këtë rast është i posaçëm; kur vepra penale kryhet në bashkëpunim; kur vepra penale kryhet më shumë se një herë; kur vepra penale ka sjellë pasoja të rënda për interesin publik.

Vepra penale "Hyrje e paautorizuar kompjuterike" është sanksionuar në nenin 192/b[87] të Kodit Penal të Republikës së Shqipërisë.

Kjo dispozitë është vendosur në Kreun VIII të Pjesës së Posaçme të Kodit Penal, ku parashikohen vepra penale për falsifikimin e dokumentave dhe është hartuar në përputhje me atë që kërkohet nga Konventa e Budapestit. Sanksionimi i një dispozite të tillë u bë tejet i rëndësishëm për mbrojtjen nga aksesi i paautorizuar në sisteme kompjuterike private apo shtetërore, gjë e cila ndihmon drejtpërdrejt edhe në mbrojtjen e të dhënave kompjuterike nga ndryshimi apo shkatërrimi si pasojë e sulmeve kompjuterike.

Objekti i veprës penale janë marrëdhëniet juridike të vendosura për garantimin e sigurisë së sistemeve kompjuterike qofshin ata private, publike apo dhe ushtarake.

Nga ana objektive krimi kryhe në mënyra të ndryshme, të cilat sjellin si pasojë hyrjen e paautorizuar ose tejkalimin e kompetencave për të hyrë në një sistem kopjuterik. Kjo dispozitë e vendos theksin te pasojat që vijnë nga veprimet e ndyshme, të cilët duhet të cënojnë masat e sigurisë.

Subjekti mund të jetë i përgjithshëm ose i posaçëm. Pra, çdo person mund të hyjnë në mënyrë të paautorizuar në një sistem kompjuterik dhe ngarkohet me përgjegjësi penale nëse nuk gëzon ndonjë nga elementët të cilët të përjashtojnë nga përgjegjësia penale sipas legjislacionit penal. Subjekti është i posaçëm në ato raste kur personi ka autorizim për të kryer një ose disa veprime duke ndërhyrë në një sistem kompjuterik të caktuar por ai e tejkalon këtë autorizim duke kryer veprime të cilat nuk parashikohen nga autorizimi.

87 Neni 192/b i Kodit Penal - **Hyrje e paautorizuar kompjuterike**
"Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet."

Nga ana subjektive vepra penale kryhet me dashje të drejtpërdrejtë dhe ka qëllim cënimin e masave të sigurimit për të pasur akses në një sistem kompjuterik pa autorizim.

Në paragrafin e dytë të kësaj dispozite parashikohen si rrethana cilësuese kur kjo vepër penale kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo çdo sistemi tjetër kompjuterik me rëndësi publike. Në përcaktim e rrethanave cilësuese legjislatori ka mbajtur në konsideratë intersi publike dhe pasojat që mund të shkaktojë hyrja e pautorizuar në këto sisteme kompjuterike.

8. Problematikat kryesore që hasen nga shtetet në luftën kundër krimit kompjuterik

Bashkëpunimi ndërkombëtar është një nga elementët më të rëndësishëm për parandalimin dhe goditjen e krimit kibernetik, duke pasur parasysh natyrën e veçantë që kanë krimet kompjuterike. Në ditët e sotme, shumica e shtetve është bindur se veprimtaria kriminale kibernetike nuk mund të luftohet e aq më pak të mposhtet duke luftuar vetëm. Por pavarësisht këtij ndërgjegjësi dhe krijimit të shumë instrumenteve kombëtarë dhe një një instrumenti ndërkombëtarë si EUROPOL, ende shtetet hasin një sër problemesh gjatë bashkëpunimit në luftën kundër krimit kibernetik. Ka qënë pikërisht, Qendra Europiane e Europolit për Krimet Kiberneti, e cila në Raportin e saj të Vlerësimit të Kërcënimit të Krimit Kibernetik[88], nxjerr në pah problematikat dhe sfidat kryesore në luftën kundër krimit kibernetik.

Kuadri ligjor kombëtar shikohet si një nga problemet kryesore. Parashikimet ligjore ndryshojnë midis vendeve në Evropë, duke e bërë hetimin efektiv ndërkufitar dhe ndjekjen penale të krimit kibernetik jashtëzakonisht të vështirë. Dallimet kryesore lidhen me atë se cila sjellje parashikohet nga çdo legjislacion si sjellje kriminale dhe procedurat që ndiqet nga vendet për kryerjen e hetimeve. Kjo e fundit ka një ndikim të madh në mbledhjen e provave elektronike dhe monitorimin e aktiviteteve kriminale online, të cilat janë kritike për çdo hetim të krimit kibernetik.

Pengesat e ndryshme për bashkëpunimin ndërkombëtar. Përderisa dallimet në legjislacionet e brendshme të çdo vendi krijojnë sfida për bashkëpunim

88 EUROPOL në Raportin e vitit 2019 ka paraqitur në mënyrë të detajuar të gjitha problematikat dhe vështirësit që hasin shtetet në luftën kundër krimit kompjuterik. Për më tëpër shih në tërësi raportin e EUROPOL, https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf

ndërmjet shteteve anëtare evropiane, mungesa e një kuadri të përbashkët ligjor në mbarë botën paraqet sfida të rëndësishme për bashkëpunimin ndërkombëtar në përgjithësi. Kjo është veçanërisht problematike në rastin e sulmeve kibernetike në shkallë të gjerë që shtrihen në shumë kontinente. Në koto raste, ndihma e ndërsjellë juridike është e ngadaltë dhe joefektive, me provat që shpesh nuk sigurohen në kohë për të siguruar suksesin e një çështjeje penale. Nga ana tjetër, kriptimi është një tjetër mjet i përdorur nga kriminelët për të shmangur mundsinë që të dhënat inkriminuese të vendosen në dispozicion të autoriteteve të zbatimit të ligjit. Përdorimi i kriptomonedhave si Bitcoin i lejon kriminelët të marrin të ardhurat e krimit duke ruajtur anonimiteti.

Humbja e vendndodhjes së kryerjes së krimit kibernetik. Ky fakt ngre problematika komplekse juridiksionale lidhur me faktin se cili shtet është përgjegjës për kryerjen e hetimeve. Në raste të tilla, Konventa e Budapestit tenton të jap një rregullim mbi çështjen e juridiksionit duke ndërthurur teorinë e territorialitetit me atë të kombësisë[89].

Pamundësia per të pasur akses në të dhëna të cilat janë të rëndësishme në një hetim penal. Shpesh herë, organet e vendeve të ndryshme që janë duke hetuar një krim kibernetik, janë në gjendje të aksesojnë vetëm një gamë të kufizuar të të dhënave për shkak të ndryshimeve legjislative dhe sovranitetit territorial të vendeve të ndryshme.

Mungesa e krijimit të një partneritetit të shëndetshëm publik-privat. Sektori privat shpesh mban çelësat për t'i siguruar zbatimit të ligjit të dhëna thelbësore për të lehtësuar hetimet dhe mund të luajë një rol kyç në ndihmën për të çmontuar infrastrukturat kriminale. Pavarësisht rëndësisë së bashkëpunimit publik-privat, nuk ka një kuadër ligjor që përcakton se si

89 Neni 22 i Konventës së Budapestit parashikon: "*1. Secila Palë merr masa të tilla legjislative ose të tjera, që janë të nevojshme për të caktuar juridiksionin për çdo vepër penale të kryer në pajtim me nenet 2 –11 të kësaj Konvente, kur një vepër e tillë kryhet: a) në territorin e tij; ose b) në bordin e një anijeje që mban flamurin e asaj Pale; ose c) në bordin e një avioni të regjistruar sipas ligjit të kësaj Pale; ose d) nga njeri prej shtetasve të saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer ose nëse vepra është kryer jashtë juridiksionit territorial të çdo Shteti. 2. Secili Shtet mund të rezervojë të drejtën për të mos zbatuar ose për të zbatuar vetëm në raste të caktuara ose kushte të caktuara rregullat juridiksionale të parashikuara në paragrafët (1)b – (1)d të këtij neni ose të ndonjë pjese të tyre. 3. Secila Palë merr masa të tilla që janë të nevojshme për të caktuar juridiksionin mbi të gjitha veprat penale të përmendura në nenin 24, paragrafi (1) i kësaj Konvente, në rastet kur kryrësi i prezumuar i veprës penale është prezent në territorin e saj dhe ajo nuk e ekstradon atë tek një Palë tjetër, kryesisht mbi bazën e shtetësisë së tij/saj pas kërkesës së bërë për ekstradim. 4. Kjo Konventë nuk përjashton asnjë juridiksion penal të ushtruar në pajtim me ligjin vendas.*

5. Nëse më shumë se një Palë pretenton juridiksionin mbi një vepër që prezumohet e kryer në pajtim me këtë Konventë, Palët e interesuara, kur është e përshtatshme, bëjnë një konsultë për të përcaktuar juridiksionin më të përshtatshëm për të bërë ndjekjen penale."

sektori privat mund të bashkëpunojë me organet e zbatimit të ligjit, ndërkohë që sigurohet që ata të mos shkelin privatësinë ose të drejtat e klientëve të tyre[90].

9. Konkluzione dhe Rekomandime

Krimi kibernetik kuptohet si akt kriminalë ku kompjuterët dhe rrjetet janë shënjestër kryesore, përdoren si mjete për të kryer vepër penale ose janë vendndodhja e krimit.

Krimi kibernetik është i ndryshëm nga krimi tradicional dhe mjaft kompleks. Ai nuk njeh kufij gjeografik dhe kryhet nga individ të arsimuar të cilët kanë njohuri të thelluara mbi funksionimin e kompjuterit dhe internetit.

Duke qënë se fusha e kibernetikës është një fushë dinamike dhe në ndryshim të vazhdueshëm, instrumentat ndërkombëtar dhe ato kombëtar të ngarkuar me detyrën për të luftuar veprimtaritë kriminale ndeshen me një shumëllojshmëri sulmesh kibernetike.

Faktorët të cilët shtyjnë një individ në kryerjen e një krimi kompjuterik janë të ndryshëm, por studimi i tyre konsiderohet si element mjaft i rëndësishëm per të evidentuar dhe zbuluar autorët e këtyre krimeve.

Shtetet e Bashkuara tëAmerikës dhe Mbretëria e Bashkuar janë vende të cilat kanë miratuar më shumë ligje specifike kibernetike se çdo vend tjetër, duke krijuar një sistem ligjor të plotë për të luftuar krimin kibernetik.

Pothuajse në çdo shtet të botës, duke përfshirë këtu dhe vende si India e Australia, ndryshimet ligjore të viteve të fundit i kanë përmirësuar ndjeshëm parashikimet ligjore lidhur me krimet kibernetike, duke i ofruar kështu institucioneve shtetërore më shumë instrumenta në luftën kundër kriminalitetit kompjuterik.

Veprat penal që janë sanksionuar për të garantuar sigurinë kiberneti dhe dënuar veprimet kriminale janë të shpërndara në mënyrë kaotike në seksione të ndryshme të Kodit Penal.

Në fushën e krimit kibernetik, legjislacioni penal shqiptar mund të konsiderohet si një legjislacion bashkohor dhe në përputhje me parashikimet e Konventës per Krimin Kibernetik.

Ndryshimet në vitin 2008 në legjislacionin shqiptar konsiderohen tepër të rëndësishme për mbulimin e veprimeve të ndryshme kriminale që ndodhin

90 Dennis Miralis, https://ngm.com.au/cybercrime-5-key-challenges/

në fushën e kibernetikës.

Në çdo kohë, ligjvënësit përballen me nevojën për të balancuar interesat konkurruese midis të drejtave individuale si privatësia dhe liria e fjalës, dhe nevojës për të mbrojtur integritetin e rrjeteve publike dhe private në botë.

Pavarësisht ligjeve të shumta të miratuara për të luftuar krimin kibernetik, shumë çështje komplekse ende kanë mbetur të pazgjidhura për shkak të vështirësive që hasen ndërmjet shteteve kur lind nevoja për bashkëpunimin e tyre për zbardhjen e një krimi kibernetik.

Për të garantuar sigurinë kibernetike dhe një luftë efektive kudër veprimeve të kundraligjshme në fushën kibernetike kërkohet domosdoshmërisht bashkëpunimi ndërmjet shteteve, të cilët duhet të ndërmarrin masat e nevojshme per të eleminuar problematikat që hasen gjatë bashkëpunimit ndërmjet tyre.

Pavarësisht hapave pozitiv në vendin tonë, aktualisht vihet re se mungojnë mjetet e nevojshme për të krijuar inteligjencën kibernetike të aftë për të garantuar sigurinë kibernetike. Rritja e kapaciteteve për t'u përballur me sfidat kibernetike është thelbësore pasi do të shoqërohej dhe me rritjen e nivelit të njohurive dhe aftësive të ekspertëve të fushës së kibernetikës.

Ashtu siç e theksova gjatë analizës juridko-penale të veprës penale të mashtrimit kompjuterik, në legjislacionin tonë kemi mungesë sa i përket përkufizimit të veprimeve teknike që ndërmeren gjatë kryerjes së veprave penale në fushën kibernetike. Për të patur një kuptim më të qartë të këtyre veprave penale duhet që legjislatori të bëjë plotësimet e nevojshme në Kodin Penal.

Konceptet e përdorura në fushën e krimit kibernetik janë shpesh herë mjaft specifike dhe teknike, gjë e cila i krijon vështirësi gjyqtarëve dhe prokurorëve gjatë gjykimit apo hetimit të veprave penale kompjuterike. Për këtë arsye duhet të merren masat e nevojshme për të trajnuar dhe aftësuar gjyqtarët dhe prokurorët, që të mund të ndjekin ligjërisht dhe gjykojnë me profesionalizëm krimin kibernetik.

Një hap i rëndësishëm në zhvillimin e legjislacionit dhe marrjen e masave kundër krimit kibernetik, është edhe hartimi i strategjive kombëtare për krimin kibernetik nga ana ekspertëve të fushës.

Të kryhet për sa është e mundur nënshkrimi, ratifikimi dhe zbatimi i çdo instrumenti ndërkombëtar që garnton sigurinë në internet, duke marrë në konsideratë zhvillimet teknologjike.

Qeveria duhet t'i kushtojë më shumë vëmëndje krimit kibernetik pasi ndikon në ekonominë e gjithë vendit.

Duke qënë se vendi ynë ka qënë disa herë pre e sulmeve kibernetike është e nevoshjme rritja e investimeve për të siguruar sisteme bashkohore (hardëare dhe software) për të siguruar hapsirën kibernetike.

Ndjekja e politikava për informimin dhe edukimin e shoqërisë mbi krimet kompjuterike është gjithashtu thelbësore. Shumica e sulmeve kibernetike janë të suksesshme për faktin se përdoruesit e teknologjisë së infomacionit nuk zbatojnë masat minimale mbrojtëse për shkak të mungesës së njohurive të nevojshme. Informimi i shoqërisë gjithashtu rrit sensibilizimin e çdo anëtari të saj për të kallëzuar në organet kompetente rastet e krimeve kibernetike apo dhe rastet kur është vet viktimë e një sulmi kompjuterik.

Bibliografi

Kushtetuta e Republikës së Shqipërisë.

Kodi penal i Republikës së Shqipërisë.

Kodi i Procedurës Penale të Republikës së Shqipërisë.

Ligji nr. 8888, dat 25.04.2002 "Për ratifikimin e Konventës Për Krime në fushën e Kibernetikës".

Ligji nr. 8733, "Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.01.1995, Kodi Penal i Republikës së Shqipërisë".

Ligji nr. 10023, date 27.11.2008 "Për disa shtesa dhe ndryshime në Kodi Penal i Republikës së Shqipërisë".

Ligji nr. 108/2014 "Për policinë e Shtetit".

Ligji nr. 97/2016 "Për organizimin dhe funksionimin e Prokurorisë në Republikën e Shqipërisë".

Ligji nr. 42/2021 "Për disa shtesa dhe ndryshime në ligjin nr. 97/2016 "Për organizimin dhe funksionimin e Prokurorisë në Republikën e Shqipërisë".

Konventa për Krimin Kibernetik.

Ligji nr. 9262, datë 29.07.2004 "Për ratifikimin e " Protokollit shtesë të konventës për krimin kibernetik, për penalizimin e akteve me natyrë racise dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike".

Vendimit nr. 673, datë 22.11.2017 "Për Riorganizimin e Agjencisë

Kombëtare të Shoqërisë së Informacionit”

VKM Nr. 1084, datë 24.12.2020, “Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të veprimit 2020-2025”.

Ligji nr. 2/2017, “Për sigurinë kibernetike”.

Ligji nr. 9918, datë 19.5.2008, “Për komunikimet elektronike në Republikën e Shqipërisë”, i ndryshuar.

Ligji nr. 9887, datë 10.3.2008, “Për mbrojtjen e të dhënave personale”, i ndryshuar.

Vikki Davies - The history of cybersecurity | Cyber Magazine.

Avokat Parvez Mirza - Cyber stalking, Cyber Harassment and Cyber Bullying – Astrea Legal Associates LLp.

Aabha Bara - What is Cyber Defamation? - LawLex.Org.

Javeline Strategy & Reasearch - Identity Fraud Losses Total $52 Billion in 2021, Impacting (globenewswire.com).

UNODC - Cybercrime Module 2 Key Issues: Offences against the confidentiality, integrity and availability of computer data and systems (unodc.org).

Kërkues Ritu – “Cyber crimes National and International prespective”. Shodhganga@INFLIBNET: Cyber crimes National and International perspective

Ajeet Singh Poonia, Dr. Awadesh Bhardwaj, Dr. Dangaya’ch - “Cyber Crime, practices and policies for its prevention” Cyber Crime: Practices and Policies for Its Prevention - DocsLib.

National Crime Agency – “Pathways into cyber crime” file (nationalcrimeagency.gov.uk).

Dr. Michael McGuire – “Into the web of profit” INTO THE WEB OF PROFIT - SecureTheVillage.

The Black Report 2018 report_nuix_black_report_2018_web_us.pdf (hubspot.net).

Jitender K Malik dhe Dr. Sanjaya Choudhury – “Law relating to cyber crimes – Comparative perspective” (PDF) Law Relating to Cyber Crimes-Comparative Perspective (researchgate.net).

Ms Jyoti Jain & Ms Rashmi Chaudhary – “Understanding the concept

of cyber crime in India vis-à-vis cyber law of USA", https://www.ijrar.org/papers.

Louise Howland – " A guide to UK cybercrime legislation" Cybercrime Legislation UK | Computer Misuse Act | ramsac.

Communication Act 2003.

Legislation.gov. uk, Investigatory Powers Act 2016 (legislation.gov.uk).

Cybercrime Act 2001, Microsoft Word - Cybercrime2001.doc (coe.int).

Kodi penal i Australis 1995, Criminal Code Act 1995 (legislation.gov.au).

Ligji i Sigurisë së Infrastrukturë Kritike të Australi 2018, Security of Critical Infrastructure Act 2018 (legislation.gov.au).

Eurojust and Europol – "Common challenges in combatin cybercrime " https://www.europol.europa.eu/sites/default/files/documents/common_challenges_in_ combating_cybercrime_2018.pdf

Denis Miralis – " Cybercrime issues and challenges" The 5 key challenges for law enforcement in fighting cybercrime | NGM Lawyers

Aldo Shkembi – " Krimi kibernetik, harmonizimi i legjislacionit shqiptar me atë Europian" https://uet.edu.al/wp-content/uploads/2021/11/Aldo_Shkembi.pdf

Joseph, Aghatise E. (28 June 2006). "Cybercrime definition". www.crime- research.org.

Shodhganga – "Meaning, Concept and Classification of Cyber Crime" https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha%5bpter%203.pdf

Edward Mercer – "Causes of Cyber Crime" <https://itstillworks.com/causes-cyber-crime-1846.html>

Parthasarathi Pati, "Cyber crime" https://www.naavi.org/pati/pati_cybercrimes_dec03.htm

CYBERSTALKING - THE NECESSITY OF ADOPTING AN AD HOC CRIMINAL PROVISION, TO ENSURE AN EFFECTIVE PROTECTION OF VICTIMS IN THE DIGITAL AGE

ROJMIR HAMZAJ[1]
rojmirh@yahoo.com.

FJORISA SHARKU[2]
fjorisasharku@yahoo.com.

Abstract

The evolution of technology and its increasing use, especially in the last decade, has led to the shift of all human relationships in the digital world, including pathological forms of interaction. This has given more space to new criminal situations such as stalking, which when transferred and developed on social networks or other digital platforms, means replacing acts of harassing someone in the street with similar behavior, but in an

1 *Rojmir Hamzaj completed his studies at the University of Trieste in Italy. He has been an attorney since 2012 and is actually practicing law at the law firm "Rojad". He has also been engaged as a lecturer of "Medical Legislation" at the Faculty of Medical Sciences, Tirana University of Medicine. Author of several scientific papers. E-mail* rojmirh@yahoo.com.

2 *Fjorisa Sharku has completed a scientific master's degree in Criminal Law at the Faculty of Law, University of Tirana. She is currently practicing law at the Ministry of Health and Social Protection. E-mail:* fjorisasharku@yahoo.com.

almost limitless space, called cyberstalking.

This new figure of stalking, carried out through the use of technology, is the object of analysis in this short scientific paper. This paper focuses initially on the causes that lead the perpetrator to commit these criminal acts and the consequences they bring to the victim, to continue with the identification of the legal framework in force for the protection of these victims, concluding with a comparative analysis of how this phenomenon is defined in Albanian and foreign doctrine and jurisprudence. Of course, special attention in this paper is dedicated to the recent innovations on this crime figure by the European Court of Human Rights which, in the opinion of the authors, is the premise for a further modernization of our Criminal Code, modernization which is possible through the formulation of a new ad hoc provision of cyberstalking or otherwise reformulation of the provision in force, provided in Article 121/a of the Criminal Code of the Republic of Alba

Key Words: cyberstalking, prosecution, victim protection, legal provisions, ECHR

1. Cyberstalking

Njerëzit kanë pothuajse të njëjtat dëshira, emocione dhe mundësi për të shprehur ose jo sjellje devijuese si në botën reale ashtu dhe në atë virtuale. Por, ndërthurja e realitetit me atë të fantazisë që japin rrjetet sociale, mund të rrisë obsesionin e një individi për të krijuar situata të rrezikshme përndjekje([3]). Sipas një përkufizimi([4]), me termin "*cyberstalking"* nënkuptohet sjellja ngacmuese e autorit i cili, duke përdorur internetin apo instrumente të tjera të ngjashme, ndërhyn në mënyrë të përsëritur, të padrejtë dhe të palejuar në sferën e jetës private të një personi, duke i shkaktuar atij një gjendje të rëndë ankthi, stresi dhe frike. *Cyberstalker,* shpesh rezulton të jetë një person me një inteligjencë të caktuar dhe të ketë njohuri të avancuara kontrolli, zotërimi dhe përdorimi të pajisjeve informatike, edhe pse në shumë raste ai paraqet papjekuri në veprimet që kryen dhe pasiguri për të ndërtuar lidhje të qëndrueshme në jetën e përditshme apo reale. Ndaj, autori zgjedh që t'a

3 Shih L. De Fazio dhe C. Sgarbi "*Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno di cyberstalking"* në, Rasagna Italiana di Criminologia anno VI. N.3. 2012, fq. 153.

4 Shih Basu, S&Jones, R.P (2008). Regulating cyberstalking, In Schmaleger, E&Pittaro, M.L., (Eds) Crimes of the interenet (pp. 141-165. Upper Saddldel River, Nj: Prentice Hall, cituar nga A. Di Maio & D. La Muscatella në "*Il fenomeno di cyberstalking dopo la Novella legislative n. 119 del 2013: recenti questioni cocio- criminologiche ed attuali contrasti dogmatici",* në Rasegna Italiana di Criminologia, Anno XII N. 1. 2018, fq. 47.

kryejë krimin në rrjetet sociale, në chat, në forumet online, por edhe nëpërmjet përdorimit të mjeteve tradicionale si e-mail apo dërgimi i mesazheve me aparat celular. Veprimet e përndjekësit dixhital, apo cyberstalker, janë të llojeve dhe mënyrave të ndryshme por qëllimi është i njëjtë, pasi ato kryhen për të goditur viktimën dhe shkaktuar asaj gjendje të rënduar stresi, frike dhe ankthi me anë të ngacmimeve apo kërcënimeve.

Disa nga këto veprime ([5]), mund të jenë:

- *postimi i komenteve të vrazhda, fyese ose sugjeruese në internet ndaj viktimës,*
- *ndjekja e viktimës në internet duke u bashkuar me të njëjtat grupe dhe forume,*
- *dërgimi i mesazheve ose email-ve kërcënuese, kontrolluese ose të turpshme tek viktima,*
- *përdorimi i teknologjisë për të kërcënuar ose shantazhuar viktimën,*
- *etiketimi i vazhdueshëm dhe i tepërt i viktimës në postime, edhe nëse nuk kanë të bëjnë fare me të,*
- *komentimi ose pëlqimi i gjithçkaje që viktima poston në internet,*
- *krijimi i llogarive të rreme për të ndjekur viktimën në mediat sociale,*
- *dërgimi i mesazheve viktimës në mënyrë të përsëritur,*
- *hakerimi ose vjedhja e llogarisë në internet viktimës,*
- *përpjekje për të patur marrëdhënie seksuale me viktimën ose dërgimi i fotove me përmbajtje të tillë viktimës,*
- *dërgimi i dhuratave ose sendeve të padëshiruara viktimës,*
- *shpërndarja e informacioneve konfidenciale në internet,*
- *postimi ose shpërndarja në internet e fotove të vërteta ose të rreme të viktimës,*
- *dërgimi i përsëritur i fotove apo videove me përmbajtje seksuale tek viktima,*
- *shpërndarja e fotove apo videove me natyrë seksuale në rrjetet sociale apo mjetet e tjera dixhitale,*
- *krijimi i postimeve të rreme, të krijuara enkas për të turpëruar viktimën,*

5 Shih në faqen elektronike https://www.verywellmind.com/what-is-cyberstalking-5181466 aksesuar për herë të fundit më datë 6.8.2022.

- *ndjekja e lëvizjeve të viktimës në internet duke instaluar pajisje gjurmuese,*
- *hakerimi në pajisjet elektronike të viktimës, veçanërisht në kamerën e laptopit apo smartphone-it të saj, si një mënyrë për t'a regjistruar dhe filmuar fshehurazi atë.*
- *vazhdimi i sjelljeve ngacmuese edhe pasi nga viktima t'i jetë kërkuar ndalimi.*

Nëpërmjet këtyre veprime dhe pa patur asnjë kontakt fizik me viktimën, përndjekësi përpiqet, dhe shpeshherë arrin me sukses, t'a kontrollojë viktimën dhe t'i shkaktojë asaj gjendje frike, ankthi dhe pasigurie.

Sipas një studimi([6]) ka rezultuar se *cyberstalker* janë:

- *kryesisht single (52.3%);*
- *me njohje informatike të mesme – të lartë (60%);*
- *me një punësim të qëndrueshëm (50%);*
- *me një diplomë gjimnazi ose universiteti (50%).*

2. Pasojat e përndjekjes online tek viktima

Ashtu si përndjekja apo "*stalking*", ndjekja online ose dixhitale ka potencialin të shkaktojë një gamë të gjerë pasojash fizike dhe emocionale për ata që janë në shënjestër. Viktimat e përndjekjes kibernetike janë përgjithësisht femra, me të cilat autori mund të ketë patur një njohje të thjeshtë ose diçka më tepër, siç mund të jetë një njohje shoqërore apo sentimentale. Ngacmimi nis pikërisht në momentin që kjo pseudo-lidhje shoqërore apo sentimentale ndërpritet për shkak të një vendimi që merr vetë viktima. Nuk mungojnë rastet e tjera, ku autori është krejtësisht i panjohur për viktimën. Por, për shkak të lehtësive që ofron teknologjia informatike dhe dixhitale, autori arrin njësoj të krijojë njohje duke marrë informacione dhe të dhëna personale të viktimës të cilat më pas i përdor kundër saj.

Po sipas këtyre studimeve([7]) viktimat e *cyberstalker* rezultojnë të jenë:

- *të martuara ose në bashkëjetesë (76,5%)*

6 Shih studimet e kryera në vitin 2003 nga McFarlane&Bocij, në faqen elektronike https://www.unobravo.com/post/cyberstalking-relazioni-in-rete aksesuar për herë të fundit më datë 6.8.2022.

7 Shih "*Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno di cyberstalking*" në Rasegna Italiana di Criminologia, Anno. VI, Nr. 3. 2012, fq. 154 -155.

- *kryesisht studentë (21%),*
- *me një diplomë unversiteti të nivelit të parë (50%),*
- *me njohje informatike të mesme.*

Sa i përket numrit të viktimave të përndjekjes dixhitale, mund të thuhet se kohët e fundit është në shifra alarmuese. Sipas një raporti amerikan([8]) numri i të rriturve amerikanë që kanë patur të paktën një përvojë të ngacmimit në internet, përfshirë këtu ndjekjen, kërcënimet fizike, ngacmimet seksuale dhe keqtrajtimet, renditet midis 18 dhe 37% ([9]). Kurse sipas të dhënave që vijnë nga një raport i realizuar nga instituti Eurispes([10])Italia 2017, 12.2 % e të intervistuarve kanë pranuar se kanë qënë viktimë e përndjekjes. Po sipas këtij Instituti, viktimat janë të përqendruara kryesisht në grupmoshat ndërmjet 18 dhe 44 vjeç, me një rënie midis moshës 25 dhe 34 (20%). Ndjekësit rezultuan të ishin shpesh ish-partnerë (në 37.1 % të rasteve), të njohur (17.4%) dhe kolegë (15.9%). Nga ana tjetër, kur të anketuarve u bëhet pyetja në mënyrë indirekte, kemi një rritje të rasteve të përndjekjes, ku 29.6% e të pyeturve pranon se ka njohur dikë që ka qënë viktimë e përndjekjes, një përqindje e konsiderueshme, e cila është një në tre persona. Sa i përket persekutimit apo përndjekjes online, rreth 83.3 % e të anketuarve thanë se ishin ngacmuar nëpërmjet internetit dhe telefonave celularë. Pra, siç shihet, ndryshe nga stalking, përqindja e viktimave që janë ngacmuar dhe përndjekur nëpërmjet internetit dhe/ose celularit është shumë më e lartë tek të rinjtë, 91.2% nga mosha 25 deri në 34 vjeç dhe 87.5% nga mosha 18 deri në 24 vjeç([11]).

Pasojat e sulmit të përndjekësit, me anë të përdorimit të mjeteve teknologjike, informatike apo dixhitale, ndikojnë në shëndetin mendor dhe mirëqenien e përgjithshme të viktimës. Shpesh, njerëzit që kanë qenë objektiv i këtij sulmi përjetojnë shqetësim, ankth, frikë dhe depresion. Madje, viktimat e sulmit të përndjekësit online apo dixhital mund të përjetojnë edhe çrregullime të stresit post-traumatik, të cilat mund të çojnë nderi në ide vetëvrasëse. Dhe rastet e ndodhura nuk janë të pakta.

Kështu, në vitin 2016 shtetasja italiane T. C. kreu vetëvrasje, duke u vetëvarur, për shkak të shpërndarjes në rrjetet sociale, e më gjerë, të

8 6 Shih, "*Countering Technologi-Facilitadet Abuse-Criminal Justice strategies for combating non consensual pornography, Sextortion, Doxing and Swatting*", RAND - 2020.

9 Shih, Anti-Defamation League, "*Online Hate and Harassment: The American Experience*" në https://www.adl.org/onlineharassment#survey-report

10 L'Instituto di Ricerca degli italiani, themeluar në vitin 1982.

11 Shih në faqen e internetit https://eurispes.eu/news/eurispes-rapporto-italia-2017-l875-dei-giovanissimi-e-stato-vittima-di-cyber-stalking/ aksesuar për herë të fundit më datë 9.8.2022.

disa videove private të saj me përmbajtje seksuale. Nga ai moment T.C., do të fyhej, përqeshej, përtallej, kërcënohej madje edhe kontaktohej në mënyrë të vazhdueshme nga individë të shumtë për të patur raporte apo marrëdhënie seksuale me të. Kjo video, kishte përfunduar edhe në faqet web të pornografisë. Pas tentativave të pasukseshme, megjithë rrugët ligjore të ndjekura për heqien e këtyre përmbajtjeve me natyrë seksuale nga rrjetet sociale dhe adresat e tjera të website, 31 vjeçarja po shkonte drejt depresionit të rëndë. Ajo ndihej gjithmonë e më shumë e turpëruar, e dëshpëruar, e vetmuar dhe e pafuqishme për të vazhduar më tej jetën e saj normale. Kjo gjendje psikike dhe fizike e rënduar do të çonte T.C., drejt vetëvrasjes ([12]). Edhe pasi kishte kaluar kohë nga kjo ngjarje tragjike, në vitin 2021 do të shpërndahej në një website amerikan sërisht e njëjta video me përmbajtje seksuale, që pasqyronte viktimën([13]). Pas kësaj ngjarje, por edhe duke marrë shkas nga rritja e konsiderueshme e këtij fenomeni, ligjvënësi italian në vitin 2019 miratoi ligjin mbi "*Revenge porn"*([14]).

Ky fenomen, me këto pasoja tragjike, është hasur edhe në mjaft vende të tjera. Kështu, në Kanada një pesëmbëdhjetë vjeçare do të vetëvritej në vitin 2012, duke u vetëvarur në dhomën e saj të gjumit. Kjo, për shkak të shpërndarjes online nga një person të imazheve të saja me përmbajtje seksuale. Pas shpërndarjes së këtyre fotografive, e mitura ra në një gjendje ankthi, frike dhe depresioni. Në shkollë ajo ofendohej, tallej, përqeshej, fyhej, kërcënohej dhe ngacmohej. Për këtë ajo mendoi të ndryshonte shkollën, duke u regjistruar në një shkollë tjetër. Por, pas një viti shfaqet në Facebook një profil me emrin e saj. Faqja kishte një foto profili me gjoksin e saj dhe me një numër të konsiderueshëm shokësh të rinj virtual të cilët përdorën një gjuhë urrejtje, përçmimi dhe neverie ndaj të miturës. Madje, duke e konsideruar të miturën një person të pamoralshëm, një grup të rinjsh e dhunuan fizikisht atë. Pas këtij momenti, e mitura ndodhur e braktisur, e dhunuar, e bullizuar, dhe e kërcënuar tenton disa herë të vetëvritet, deri kur në vitin 2012 gjen vdekjen([15]).

---

12 Shih në faqen e internetit, https://notizie.virgilio.it/tiziana-cantone-storia-ultime-notizie-1498093 aksesuar për herë të fundit më datë 8.8.2022.

13 Shih në faqen e internetit, https://napoli.repubblica.it/cronaca/2022/05/18/news/tiziana_cantone_video_napoli-350102095/ aksesuar për herë të fundit më datë 8.8.2022.

14 Shih në faqen e internetit https://www.diritto.it/il-reato-di-revenge-porn aksesuar për herë të fundit më datë 8.8.2022. Me ligjin e datës 19 korrik 2019 n. 69, parashikohet shprehimisht në nenin 612 ter K.Penal vepra penale e "*Revenge porn*" titulluar " *Shpërndarja e paligjshme e imazheve ose videove me përmbajtje seksuale*".

15 Shih në faqen e internetit, www.bbc.co.uk/newsbeat/article/19960162/amandatodd-memorial-for-teenage-cyberbullying-victim aksesuar për herë të fundit më datë 8.8.2022.

Po në këtë periudhë, në Kanada do të vetëvritej edhe një e mitur tjetër shtatëmbëdhjetë vjeçare([16]), e cila kishte tentuar disa herë më parë vetëvrasjen. Kjo për shkak të *bullying* dhe *cyberbulling* që ushtrohej ndaj saj. E mitura e quajtur R.P., përndiqej sistematikisht, nga individë apo grupe individësh, të cilët i dërgonin mesazhe të ndryshme, me anë të rrjeteve sociale apo website-ve, me propozime për takime dhe kryerje të marrëdhënieve seksuale. Mesazhet shpesh përmbanin përçmim, sharje, ngacmime, tallje dhe kërcënime në rast refuzimi në kryerjen e marrëdhenieve seksuale.

Një tjetër rast i *cyberstalking* dhe *cyberbulling*([17]) që do të shqetësonte jo pak autoritetet braziliane dhe mbarë opinion publik, ishte edhe vetëvrasja e shtatëmbëdhjetë vjeçares J.R. Kjo e fundit u gjet e vetëvarur në vitin 2013 në Piaui të Brazilit. Shkak ishin ngacmimet dhe kërcënimet sistematike që i bëheshin nga ish i dashuri, me anë të mjeteve informatike dhe shpërndarja më pas online e një video me përmbajte seksuale ku pasqyrohej viktima. Disa javë para këtij gjesti ekstrem e mitura kishte shkruar për prindërit e saj ,"*Më falni që nuk jam një vajzë perfekte. Shumë shpejt çdo gjë do të mbarojë".*

Këto fenomene në rritje, të *cyberstalking, cyberbulling* dhe "*revenge porn*", sollën një ndërgjegjësim të rëndësishëm jo vetëm të shoqërisë por edhe ligjvënësve të vendeve të ndryshme, të cilët ndërhynë me urgjencë në legjislacionin penal duke parashikuar vepra penale të reja ose ndryshuar ato ekzistente, me qëllim parandalimin dhe ndëshkimin e autorëve. Ndëshkim i cili, marrë shkas nga zhvillimi i avancuar teknologjisë informatike dhe dixhitale, përdorimi masiv i këtyre teknologjive, shpejtësia në hyrjen dhe marrjen e informacioneve dhe mundësia për të krijuar apo ndërtuar relacione ndërpersonale virtuale edhe duke ndenjur anonim, bëhet gjithmonë e më i vështirë.

Kuadri ligjor shqiptar në fuqi

Ligjvënësi shqiptar nuk ka përcaktuar ndonjë dispozitë të veçantë penale për të luftuar fenomenin e "*cyberstalking"*, aq më pak atë të "*cyberbullying*" dhe "*revenge porn*". Në seksionin VII të K.Penal "*Vepra penale kundër*

16 Shih në faqen e internetit, https://www.corriere.it/esteri/13_settembre_18/facebook-usa-foto-ragazza-suicida-dopo-stupro-proteste-e-scuse_03f6e1bc-2067-11e3-8197-f40f962f8de4.shtml aksesuar për herë të fundit më datë 8.8.2022.

17 Shih në faqen e interenetit, https://www.bustle.com/articles/9485-revenge-porn-legislation-called-for-in-brazil-following-17-year-olds-suicide aksesuar për herë të fundit më datë 8.8.2022.

moralit dhe dinjitetit" listohet neni 121/a titulluar "*Përndjekja*" ku parashikohet se: "*Kërcënimi ose ngacmimi i personit me anën e veprimeve të përsëritura, me qëllimin për t'i shkaktuar një gjendje të vazhdueshme dhe të rëndë ankthi apo frike për sigurinë vetjake, të një të afërmi ose të një personi, me të cilin ka lidhje shpirtërore, apo për ta detyruar të ndryshojë mënyrën e tij të jetesës, dënohet me burgim nga gjashtë muaj gjer në katër vjet.*

Kur kjo vepër kryhet nga ish-bashkëshorti, ish-bashkëjetuesi apo personi që ka pasur lidhje shpirtërore me të dëmtuarin, dënimi rritet me një të tretat e dënimit të dhënë.

Kur kjo vepër kryhet ndaj të miturit, gruas shtatzënë ose një personi të pazotë për t'u mbrojtur, si dhe kur kryhet nga një person i maskuar ose shoqërohet me mbajtjen ose me përdorimin e armëve, dënimi rritet deri në një të dytën e dënimit të dhënë".

Kjo figurë krimi është miratuar me ligjin n. 23/2012. Përpara miratimit të kësaj dispozite, këto veprime kriminale ndëshkoheshin duke u bazuar në vepra të tjera penale të ndryshme, si ajo e "*Kanosjes*" parashikuar në nenin 84; "*Plagosje e rëndë", " Plagosja e lehtë" dhe "Dëmtime të tjera me dashje"* parashikuar në nenet 88, 89 dhe 90 - kur viktima për shkak të këtyre veprimeve me dashje të autorit pësonte ankth, frikë dhe stres (*pasoja tipike të kanosjes*) apo dëmtim, të rëndë apo të lehtë, në shëndetin e saj; "*Përhapja e sekreteve private*" parashikuar në nenin 122 – ku autori përhap me dashje një sekret të jetës private të një personi tjetër; "*Prishje e qetësisë publike*" parashikuar në nenin 274 - ku integron elementët e kësaj vepre penale edhe çdo lloj sjellje tjetër e papëlqyeshme e kryer në rrugë, sheshe a mjedise publike, që cënon dukshëm qetësine e moralin e personit, dhe "*Përdorimi me keqdashje i thirrjeve telefonike*" parashikuar në nenin 275 - që bëhen me dashje nga autori për të prishur qetësinë e tjetrit.

Mirëpo, inkuadrimi i këtyre sjelljeve të autorit jo në një vepër penale të vetme por në disa të tilla dhe më pak të rënda, bënte që viktima të mos kishte një mbrojtje adekuate. Pasi, sjelljet e autorit përndjekës paraqitnin një rrezikshmëri më të madhe se ato të veprave të tjera të sipërcituara, jo vetëm për shkak të përsëritjes së tyre dhe qëllimit që kanë, por edhe për efektet tejet negative që ato shkaktojnë në sferën e jetës private dhe familjare të personave të dëmtuar.

Nga ana tjetër, represioni penal ndaj përndjekësit nuk mund të bazohej në formulime ligjore të diktuara për vepra penale të tjera apo të ngjashme me atë të përndjekjes. Bazuar në parimin e ligjshmërisë, konkretisht atë të

përcaktimit, ([18]) ligjvënësi është i detyruar që në formulimin e një norme penale të jetë i qartë dhe i saktë. Kjo, jo vetëm për të mos i lënë hapësirë subjektivizmit, keqkuptimit nga organet ligjzbatuese por edhe për ti dhënë mundësi shoqërisë që ajo të njihet e ta kuptojë normën penale, për të qenë kështu e vetëdijshme për veprimet apo mos veprimet e saj([19]).

Bazuar në këto konsiderata, ligjvënësi shqiptar ndërhyri në vitin 2012 në Kodin Penal duke miratuar nenin 121/a.Objekt i kësaj dispozite janë raportet juridike të vendosura për të siguruar të drejtën e çdo individi për gëzimin e qetë të jetës private dhe sociale pa kontrollin nga të tjerët. Këto raporte juridike cënohen nga ndërhyrjet e padrejta të personave të tjerë, të cilët me veprimet e tyre kërkojnë t'i heqin apo kufizojnë këto të drejta viktimës. Kjo mbrojtje, referuar mënyrës si është formuluar dispozita, synohet midis atyre personave që janë në lidhje bashkëshortore, bashkëjetuese ose çdo lidhje tjetër afektive shpirtërore.

Në vlerësimin e atij që shkruan, e mira materiale që kërkohet të merret në mbrojte nga norma penale është, përpos lirisë morale të individit kuptuar si e drejta për të vetëvendosur, edhe mbrojtja e sigurisë dhe shëndetit individual të viktimës, duke qënë se aktet e përndjekësit kanë mbi viktimën një efekt destabilizues në shëndetin, qetësinë dhe ekuilibrin psikologjik të tij. Vetëm kështu do të mbrohej viktima dhe garantohej mosizolimi i personalitetit të tij nga ndikimet shqetësuese, si frikë, stres dhe ankth, që sjellin veprimet e përndjekësit. Sipas disa autorëve të huaj, ([20]) e mira materiale e cënuar drejtpërdrejtë në rastin konkret është qetësia individuale, pra interesi i secilit individ për të jetuar i lirë nga të gjitha shqetësimet. Kurse sipas një autori tjetër([21]), kjo e mirë materiale që merret në mbrojtje nga rendi juridik është liria morale dhe psikike e viktimës, që vihet në rrezik nga kërcënimet dhe ngacmimet e përndjekësit të cilat shkaktojnë frikë dhe ankth tek ajo.

Nga ana objektive, ky krim manifestohet me anë të veprimeve të një natyre

18 Shih C. Fiore e S. Fiore në Diritto penale, Pjesa e përgjithshme, casa edittrice Torino, anno 2008, fq. 67, cituar nga R.Hamzaj në Konferencën Shkencore Kombëtare, Drejtësia Penale Shqiptare – *Mes vlerave të traditës, meritës së ndryshimeve dhe largëpamësisë së ligjit dhe shoqërisë,* "*Keqinterpretimi dhe keqzbatimi i nenit 291 të K.Penal të Republikës së Shqipërisë, shkak i ndëshkueshmërisë pa ligj të shtetasve*" fq. 94.

19 Shih F.C.Palazzo, Il pricipio di determintatezza nel diritto penale, CEDAM, Padova , fq. 5, cituar nga R. Hamzaj në "*Keqinterpretimi dhe keqzbatimi i nenit 291 të K.Penal të Republikës së Shqipërisë, shkak i dëshkueshmërisë pa ligj të shtetasve*" , po aty fq. 94..

20 Shih në faqen e internetit, https://www.diritto.it/cyberstalking-le-nuove-frontiere-del-diritto-penale/ ku citohen autorët Antolisei, Findaca- Musco, Mantovani, aksesuar për herë të fundit më datë 8.8.2022.

21 Shih në faqen e internetit , https://www.diritto.it/cyberstalking-le-nuove-frontiere-del-diritto-penale/ ku citohet autori Pisapia.

të tillë të cilat në kontekstin e sjelljeve njerëzore janë të padëshirueshme, që shkaktojnë bezdisje, apo që çojnë në situata të pakëndshme. Kjo vepër karakterizohet nga sjellje alternative dhe nga fakte jo të njëjta, por të ngjashme([22]). Veprimet kërcënuese ose ngacmuese mund të marrin forma të ndryshme. Ato mund të jenë verbale ose fizike dhe mund të bëhen veçmas ose të kombinohen. Për shkak të këtyre sjelljeve viktima ndihet e frikësuar, përjeton ankth dhe tension të cilat bëhen pengesë për të jetuar normalisht jetën e saj. Këto veprime autori mund t'i kryejë nxitur nga motivi i një afrimi reciprok, mund të jenë të nxitura nga një pëlqim, emocion dashurie, por edhe nga një urrejtje e krijuar. Kërcënimet dhe ngacmimet nuk janë të rastësishme, por të llogaritura që synojnë dëmtimin e personit tjetër ose që të krijojë një mënyrë jetese të ndryshme nga ajo që bën realisht subjekti pasiv sipas vullnetit të tij. Ankthi dhe frika e krijuar tek subjekti pasiv duhet të kenë lidhje objektive me sjelljen e personit që kundrejton sjelljen, dhe jo të jetë një gjendje e krijuar nga faktorë të tjerë apo e vetë gjendjes së të dëmtuarit. Pra, të ketë lidhje shkakësore midis veprimeve të autorit dhe pasojës së ardhur viktimës.

Një element tjetër i detyrueshëm pa të cilin nuk jemi në kushtet e përndjekjes është që veprimet kërcënuese dhe ngacmuese duhet të jenë të përsëritura. Me termin *"të përsëritura"* do të nënkuptohet se autori në mënyrë të vazhdueshme e ribën të njëjtin veprim, por midis ngjarjeve duhet të ketë lidhje. Në këto përsëritje megjithëse faktet mund të mos jenë të ngjashme midis tyre, ato janë rezultat i një mendimi të vetëm kriminal. Sjelljet e përsëritura të ndodhura në vazhdimësi, duhet të kenë të njëjtën natyrë dhe të formojnë një fakt të përbashkët në tërësinë e tyre([23]).

Subjekt i veprës penale, sipas paragrafit të parë dhe të tretë të nenit 121/a, mund të jetë çdo person, i cili rezulton të ketë mbushur moshën për përgjegjësi penale. Ndërsa sipas paragrafit të dytë, subjekti është i posa 135ëm, pasi flitet për ish bashkëshort, ish bashkëjetues si dhe person që ka patur lidhje shpirtërore me të dëmtuarën.

Nga ana subjektive, krimi i përndjekjes kryhet me dashje direkte. Autori me veprime të përsëritura, të ndërgjegjshme dhe të vetëdijshme dëshiron një pasojë të caktuar e cila për rastin konkretizohet në shkaktimin e një gjendjeje të rëndë ankthi dhe frike të viktimës.

Ligjvënësi shqiptar, në formulimin e kësaj dispozite është referuar në

22 Shih Av. Agim I. Tartari, Revista "*Avokatia*", nr.22, fq. 74 cituar nga D. Mecani, e Drejta penale e posaçme, fq. 217-218.

23 Po aty, fq. 219.

parashikimet e ligjvënësit italian([24]). Por, ndryshe nga ky i fundit, ai nuk ka bërë një ndërhyrje të mëvonëshme për të krijuar një normë penale të veçantë për krimin e *cyberstalking* ose duke e parashikuar atë, të paktën si rrethanë rënduese në të njëjtën dispozitë([25]). Në formulimin e nenit 121/a shohim që ligjvënësi ka përdorur termin "*veprime përsëritëse*". Pra, lë të kuptohet që kjo vepër mund të kryehet vetëm me veprime dhe jo me mosveprime. Po ashtu, ligjvënësi nuk ka parashikuar numrin e këtyre veprimeve përsëritëse të pranishme për të integruar elementët e veprës penale. Por, përdorimi i termit "*përsëritëse*" lë të kuptohet që duhet të jenë të paktën dy veprime të tilla të kryera nga ana e autorit. Nga ana tjetër, ligjvënësi nuk shpjegon nëse do të bien në rregullimin e kësaj dispozite edhe ato veprime ngacmuese të cilat kryhen me anë të përdorimit të mjeteve informatike apo dixhitale. Praktika gjyqësore, siç do të analizohet në vijim, ka mbajtur një qëndrim pranues, duke ndëshkuar për veprën penale të parashikuar në nenin 121/a të Kodit Penal edhe ato sjellje të autorit përndjekës i cili për të arritur qëllimin përdorte internetin apo mjete të tjera të ngjashme të komunikimit elektronik.

Në vlerësimin e atij që shkruan, nuk ka qenë ky qëllimi i ligjvënësit. Ndryshe, ky i fundit në formulimin e dispozitës do të kishte përdorur shprehjen "*kur ky veprim kryhet me anë të përdorimit të mjeteve informatike apo dixhitale..",* ashtu sic rezulton e formuluar kjo dispozitë edhe në shumë legjislacione të tjera demokratike. Dhe kjo është e kuptueshme, pasi

---

24 Art. 7. Modifiche al codice penale 1. Dopo l'articolo 612 del codice penale e` inserito il seguente:

«Art. 612-bis (Atti persecutori):

Salvo che il fatto costituisca piu' grave reato, e' punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumita' propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

La pena e' aumentata se il fatto e' commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa.

La pena e' aumentata fino alla meta' se il fatto e' commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilita' di cui all'articolo 3 della legge 5 febbraio

1992, n. 104, ovvero con armi o da persona travisata.

Il delitto e' punito a querela della persona offesa. Il termine per la proposizione della querela e' di sei mesi. Si procede tuttavia d'ufficio se il fatto e' commesso nei confronti di un minore o di una persona con disabilita' di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonche' quando il fatto e` connesso con altro delitto per il quale si deve procedere d'ufficio.».

25 Shih T. Padovani në, "*L'assenza di coerenza mette a rischio la tenuta del sistema"*, in *Guida diritto*, anno 2019, f. 37, fq 51-54. Sipas autorit, për të kontrastuar krimet e reja që vijnë për shkak të përdorimit të internetit apo mjeteve të ngjashme me të, është pa dyshim e nevojshme marrja e masave urgjente për formulimin e një dispozite ad hoc për secilën nga llojet e veprimeve kriminale të stalking, cyberstalking, bullying, cyberbullying e revenge porn.

elementët e veprës penale të përndjekjes, për të cilat flet neni 121/a i Kodit, vërtet janë të njëjta me ato të përndjekjes informatike apo telematike, por mënyra e kryerjes së veprimit është e ndryshme. Në rastin e parë, kemi të bëjmë me formën tradicionale apo klasike të përndjekjes, ku ish-partneri, ish-bashkëjetuesi apo person tjetër i lidhur shpirtërisht me viktimën është i shtyrë nga dëshira për të patur një kontakt fizik me këtë të fundit apo një përballje. Për të realizuar kontaktin, autori e ndjek viktimën duke i shkuar në ambjentin e punës, studimit, dëfrimit apo banimit. E kundërta, ndodh në rastin e dytë të përndjekjes informatike apo telematike, ku autori ka një qasje vetëm virtuale me viktimën. Kjo qasje, në të shumtën e rasteve, është pikërisht për të shmangur një përballje apo kontakt fizik me viktimën. Nga ana tjetër, në përndjekjen informatike apo telematike/dixhitale problem jo i vogël është edhe përcaktimi i vendit të kryerjes së krimit([26]), pasi ndryshe nga përndjekja klasike, ai kryhet në një hapësirë virtuale të padefinuar. Në këtë rast shtrohet pyetja, se cila do të jetë gjykata kompetente për të gjykuar çështjen, ajo e vendit ku sjelljet përsëritëse janë realizuar, apo vendi ku viktimës i janë shkaktuar konkretisht pasojat (frika, ankthi, stresi) nga këto veprime të përsëritura.

Po ashtu, element tjetër që i bën këto dy fenomene të ndryshme me njëra tjetrën është edhe zbatimi i masës shtrënguese për parandalimin e kryerjes së përsëritur të veprës penale. Kështu, masa shtrënguese e ndalimit apo e detyrimit për të qëndruar në një vend të caktuar, parashikuar në nenin

26 Shih në faqen e internetit, https://www.doppiadifesa.it/wp-content/uploads/2020/06/Stalking-e-riavvicinamento_Cassazione-penale-sez.-V-sentenza-04.06.2020-n.-16977.pdf, aksesuar për herë të fundit më datë 12.8.2022. Këtij problemi, duket se i ka dhënë zgjidhje Gjykata e Cassacionit italian me vendimin n. 16977 datë 4.6.2022. Rasti ka të bëjë me ankimin e një të dënuari, në të dyja shkallët e gjykimit, për veprën penale të "*Atti persecutori*" parashikuar në nenin 612 bis të Kodit. Rekursuesi, referuar vendimeve të gjykatave të faktit, rezultonte të kishte kryer në dëm të ish – të dashurës së tij një sërë veprimesh persekutuese apo përndjekëse me qëllim që ajo të ri kthehej në lidhjen që kishin. Këto sjellje konkretizoheshin në telefonata të përsëritura ngacmuese dhe mesazhe fyese; telefonata nënës së viktimës duke i komunikuar lajmin e rremë se vajaza e saj ishte e prekur nga AIDS/SIDA;krijimin e llogarive të rremë në facebook për të komunikuar me të afërmit dhe miqtë e viktimës për të marrë informacion rreth saj; krijimi i një tjetër profili të rremë në facebook që përdorej për të shpifur për ish-të dashurën dhe atribuar asaj sjellje të rreme seksuale etj (…). Rekursuesi kërkonte prishje të vendimeve të gjykatave të faktit edhe për shkak të mos pasjes nga ana e tyre të kompetencës territoriale për të shqyrtuar cështjen. Sipas tij, gjykata kompetente do të ishte gjykata e vendbanimit të tij, nga ku ai kryente sjelljet me natyrë ngacmuese, të gjitha të kryera me anë të telefonit apo përmes rrjeteve sociale. Gjykata e lartë nuk ka pranuar këtë pretendim të rekursuesit duke argumentuar se, kompetenca territoriale përcaktohet duke parë vendin ku është konsumuar vepra penale dhe janë realizuar pasojat, pra gjendja e ankthit, frikës dhe ndryshimi i stilit të jetesës. Thënë ndryshe, duhet t'i referohemi vendit ku sjelljet e autorit bëhen të njohura dhe të kualifikueshme si persekutuese/përndjekëse dhe vendit ku shqetësimi i akumuluar nga viktima sjell gjendjen e rënduar psikike, si ankthi, frika dhe ndryshimi i mënyrës të jetesës.

232/c të K.Pr.Penale, sigurisht do t'i pamundësonte përndjekësit klasik që të vazhdonte ndjekjen e viktimës në ambientet e frekuentuara nga ana e saj. Nga ana tjetër, kjo masë do të ishte tërësisht e pazbatueshme në rastin e përndjekësit informatik apo dixhital. Pikërisht sepse ky i fundit veprimet e tij kriminale i ushtron në një platformë virtuale/dixhitale. Njëjtë, një masë sigurimi personal siç është ajo e "*Arresti në shtëpi",* parashikuar në nenin 237 të K.Pr.Penale, do të ishte e efektshme në rastin e përndjekësit klasik pasi do t'i pamundësonte atij kontaktin me viktimën, por një masë e tillë është e pazbatueshme në rastin e përndjekësit i cili vepron nëpërmjet platformës dixhitale për të kryer veprimet ngacmuese dhe kërcënuese ndaj viktimës. Edhe nën këtë masë sigurie, për autorin do të mjaftonte pasja e një pajisjeje elektronike, si pc, laptop, etj., për të realizuar përndjekjen, pse jo me një identitet të ri të panjohur për viktimën.

3. Kuadri ligjor i huaj

Në Evropë rregullimi ligjor i *stalking* nuk është i njëjtë. Shtetet si Italia, Gjermania, Austria, Irlanda, Danimarka dhe Belgjika, kanë miratuar një dispozitë *ad hoc* për të rregulluar këtë fenomen. Në formulimin e kësaj dispozite, disa nga këto ligjvënës kanë përfshirë edhe veprimet ngacmuese apo kërcënuese që kryhen me mjete informatike apo dixhitale *(cyberstalking*). Kurse shtetet e tjera, kanë ndëshkuar këtë fenomen, njësoj sikurse edhe sot, me anë të dispozitave penale të ndryshme.

Kështu, **ligjvënësi italian** me Dekret ligjin n. 11 datë 23 shkurt 2009, konvertuar me ligjin n. 38 datë 23 prill 2009, bën ndërhyrje në Seksionin III " *Krime kundër lirisë morale*", të Kreu-ut III "*Krime kundër lirisë individuale",* të Titull-it XII *"Krime kundër personit"* – duke shtuar nenin 612 - bis, i cili parashikon se: "*Salvo che il fatto costituisca piu' grave reato([27]), e' punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumita' propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.*

27 Sipas disa autorëve, kjo klauzolë është parashikuar nga ligjvënësi për shkak të ndërlidhjes që paraqesin elementët e kësaj vepre penale me veprat e tjera dhe përthithjes nga këto të fundit në rast konkurimi dhe dënimi më të rëndë, vija ndarëse e të cilave jo gjithmonë është e lehtë. Kështu shprehet, B. Romano, në *Diritto penale, Parte generale,* Terza edizione Giuffrè, Milano, 2016, fq. 494.

La pena e' aumentata se il fatto e' commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa.

La pena e' aumentata fino alla meta' se il fatto e' commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilita' di cui all'articolo 3 della legge 5 febbraio

1992, n. 104, ovvero con armi o da persona travisata.

Il delitto e' punito a querela della persona offesa. Il termine per la proposizione della querela e' di sei mesi. Si procede tuttavia d'ufficio se il fatto e' commesso nei confronti di un minore o di una persona con disabilita' di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonche' quando il fatto e` connesso con altro delitto per il quale si deve procedere d'ufficio".

Siç del nga leximi i dispozitës, ligjvënësi ka dashur të ndëshkojë të gjithë ato akte persekutuese/përndjekëse që drejtohen ndaj viktimës, duke parashikuar madje edhe një rritje të dënimit,në rastet kur përndjekja kryhet nga partneri, ish-partneri apo nga cilido person tjetër i afërt me viktimën. Por, në formulimin origjinal, ligjvënësi nuk parashikonte rastet e përndjekjes së viktimës me anë të përdorimit të teknologjisë, ndonëse ky fenomen ishte tashmë i njohur në praktikë. Megjithatë, këto raste, siç do të analizohet në vijim, njësoj do të ndëshkoheshin nga gjykata, e cila duke bërë një interpretim të zgjeruar të normës, përfundonte së trajtuari këto veprime njësoj me ato të përndjekjes klasike. Një praktikë e tillë kritikohej nga ana e doktinës, jo vetëm për shkak të interpretimit të sforcuar që i bëhej dispozitës, duke cënuar parimin e taksivitetit ([28]), që kërkon që gjykata t'i përmbahet me korrektësi dhe rreptësi ligjit ashtu siç është formuluar nga ligjvënësi, por edhe trajtimit të barabartë të këtyre dy sjelljeve, të cilat për nga kuptimi, mënyra, pasojat që shkaktojnë dhe natyra janë të ndryshme([29]).Kjo bëri, që ligjvënësi të rishikonte formulimin e mëparshëm të normës.

Kështu, me Dekret ligjin n. 93 datë 14 gusht 2013, konvertuar në ligj me aktin normativ n. 119 datë 15 tetor 2013, ndryshohet paragrafi 2 i nenit 612 bis duke parashikuar një rritje të dënimit në rastet kur sjelljet e autorit përndjekës kryhen nëpërmjet përdorimit të instrumentave informatikë apo telematikë.

Interesant është fakti që të dyja ndërhyrjet, si ajo e vitit 2009 që solli

28 Shih S. Moccia. La promessa non mantenuta. Ruolo e prospettive del principio di determintezza e tassivita nel sistema penale italiano, Edizioni scientifiche italiane – Napoli. 2001, fq 13.

29 Shih në faqen e internetit, https://www.diritto.it/cyberstalking-le-nuove-frontiere-del-diritto-penale/ aksesuar për herë të fundit më datë 9.8.2022.

miratimin e nenit 612 bis dhe ajo vitit 2013 që solli një ndryshim të paragrafit 2 të kësaj dispozite, janë bërë me Dekret ligj, instrument ky i parashikuar në kushtetutën italiane, neni 77, vetëm për rastet e jashtëzakonshme të nevojës dhe urgjences.

Në vlerësimin tonë, kjo ka ardhur për shkak të rritjes së fenomenit të përndjekjes që e bënte të pamundur shtyrjen më tej nga ligjvënësi të një rregullimi ligjor përkatës, duke ju përgjigjur kështu ndjeshmërisë publike nga njëra anë, dhe represionit, me masa më të rënda dënimi, të këtyre formave të reja të përndjekjes teknologjike, nga ana tjetër.

Arsye përse, ligjvënësi italian ndërhyn sërish([30]) në Kodin penal me ligjin n. 69/2019 titulluar *" Violenza domestica e di genere*" "*Codice Rosso*" duke shtuar ndër të tjera edhe nenin 612 - të titulluar "*Diffusione illecita di immagini o video sessualmente espliciti* " - *Revenge porn* ([31]). Vlerësojmë po ashtu se, mbi të njëjtat konsiderata që kanë çuar ligjvënësin italian të miratojë ligjin mbi "*revenge porn*" dhe atë të *"cyberbullying*" ardhur me ligjin n.71 datë 19 qershor 2017, duhej vijuar edhe me rregullimin ligjor të "*cyberstalking*", duke parashikuar një normë penale *ad hoc* ndaj këtij fenomeni. Ky do të ishte një hap përpara dhe vendimtar për garantimin e një mbrojtje të plotë të viktimave.

Rregullim i ngjashëm ligjor me atë italian haset edhe në **legjislacionin penal gjerman**. Në vitin 2007 kemi një riformulim të nenit 238 të kodit titulluar "*Nachstellung*", akte persekutuese/përndjekëse, i cili parashikon dënimin e kujtdo që:

- *me veprime të përsëritura përndjek pa të drejtë një person, duke kërkuar me insistim që të krijojë afrimitet me të,*
- *tenton të krijojë një kontakt me personin, me anë të përdorimit të mjeteve të telekomunikacionit dhe me mbështetjen e të tretëve,*
- *urdhëron mallra apo shërbime duke përdorur në mënyrë abuzive të dhënat personale,*
- *pajton një të tretë që të vihet në kontakt me viktimën.*
- *kërcënon me lëndime trupore apo cënon shëndetin dhe lirinë e viktimës*

30 Shih në faqen e internetit, https://www.sulpl.it/images/LEGGE_69-2019_CODICE.pdf aksesuar për herë të fundit më datë 9.8.2022.

31 Kjo dispozitë parashikon si vijon: "*E' punito chi, senza il consenso delle persone rappresentate, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito destinati a rimanere privati, dopo averli realizzati, sottratti ovvero ricevuti o acquistati al fine di recare loro nocumento".*

apo të një personi të afërt me të,

- *kryen veprime të ngjashme të cilat i shkaktojnë një çrregullim jetës së personit ([32]).*

Siç shihet, ligjvënësi ka përcaktuar në mënyrë shumë sintetike se cilat janë veprimet që mund të konsiderohen si akte përndjekëse apo persekutuese. Por, nga ana tjetër, duke parashikuar një klauzole mbyllëse të dispozitës, kur shprehet "*dhe sjellje të tjera ngjashme*", ligjvënësi përfundon së braktisuri metodologjinë e formulimit sintetik të normës. Në vlerësimin e atij që shkruan, vendosja e një klauzole të tillë në lëndën penale, është në kundërshtim me parimin e ligjshmërisë, konkretisht me atë të përcaktimit të normës penale. Ky parim kërkon që norma të jetë e saktë dhe e qartë. Kjo, jo vetëm për të mos i lënë hapësirë subjektivizmit, keqkuptimit nga organet ligjzbatuese por, edhe për t'i dhënë mundësi shoqërisë që ajo të njihet e t'a kuptojë normën penale, për të qenë më pas e vetëdijshme për veprimet apo mosveprimet e saja. Përdorimi i shprehjes "*dhe sjellje të tjera të ngjashme*", nuk i përgjigjet këtij parimi.

Sa i takon llojit të dënimit, ligjvënësi parashikon dënimin me gjobë ose me burg deri në tre vite. Kur për shkak të veprimeve apo ngacmimeve vihet në rrezik jeta e personit apo i shkaktohet një dëm i rëndë atij, një familjari apo personi tjetër të lidhur me të, dënimi është nga tre muaj gjer në pesë vite burgim.

Kurse në **legjislacionin austriak**, vetëm me ndryshimin në vitin 2006 të kodit penal (BGBI), do të parashikohej vepra penale e "*Beharrliche Verfolgung*", pra e përndjekjes së vazhdueshme. Në nenin 107/a të këtij kodi jepet përkufizimi i *stalking,* që konsiton në kryerjen e veprimeve të padrejta dhe të përsëritura të autorit të cilat janë të tilla që ndryshojnë mënyrën dhe stilin e jetës së viktimës për një kohë të zgjatur([33]). Veprimet e autorit janë të njëjta me ato të listuara në nenin 238 të Kodit penal gjerman, duke përfshirë edhe veprimet e kryera me anë të përdorimit të teknologjisë. Edhe këtu, sjellja e autorit duhet të jetë e përsëritur për një periudhë të gjatë kohore dhe të jetë e aftë për të kompromentuar kushtet dhe mënyrën e jetesës së viktimës. Ligjvënësi austriak nuk specifikon ndonjë numër minimal apo maksimal të veprimeve të përsëritura që do të integronin veprën penale të *stalking*. Megjithatë, nisur nga termi i përdorur "*veprime ngacmuese*

32 Shih "*Lo stalking*": *Comparazione tra le diverse esperienze giuridiche*, a cura di V. Iorio, Pegaso, Universita' telematica, fq. 14.

33 Shih "*Lo stalking*": *Comparazione tra le diverse esperienze giuridiche*, a cura di V. Iorio, Pegaso, Universita' telematica, fq. 14 -15.

të përsëritura" dhe *"me këmbëngulje"*, kuptohet se ato duhet të jenë më shumë se një herë dhe të zgjatura në kohë. Do të jetë gjykata, e cila rast pas rasti do të marrë në analizë këto fakte. Dënimi i autorit është me burg deri në një vit. Ligjvënësi, ka parashikuar po ashtu mundësinë e vendosjes së ndalimeve ndaj përndjekësit, me qëllim mbrojtjen e viktimës nga ndërhyrjet që i bëhen në jetën private.

Edhe në **legislacionin belg**([34]), që prej vitit 1998, ka një parashikim *ad hoc* të veprës penale të *stalking,* quajtur *"Belaging o harcelemente*". Neni 442 bis i kodit penal, parashikon se: "*kushdo që ngacmon një person, dhe që ishte ose duhej të ishte në dijeni që sjellja e tij cënonte qetësinë e personit tjetër , dënohet me burgim nga pesëmbëdhjetë ditë deri në dy vite burgim dhe me gjobë nga pesëdhjetë në treqind euro, ose me njërën nga këto dënime*.

Në formulimin e kësaj dispozite ligjvënësi belg, ndryshe nga ai gjerman, austriak dhe italian, nuk ka përdorur shprehjen "*veprime të përsëritura*" apo "*të vazhdueshme"*. Kjo do të thotë që, vepra penale e *stalking* do të konsiderohet e konsumuar edhe nëse përndjekësi apo ngacmuesi ka ndërmarë një veprim të vetëm ndaj viktimës. Por,ky veprim është i ndëshkueshëm vetëm nëse kërkohet të ndiqet nga viktima. Nga ana tjetër, kjo mënyrë formulimi e normës," *kushdo që ngacmon*" lë të kuptohet se në sjelljet e ndëshkueshme penalisht do të jenë edhe ato veprime ngacmuese të autorit të cilat kryhen me anë të mjeteve të teknologjisë *(cyberstalking*). Por, edhe në këtë rast një përkufizim i tillë do të ishte në kontrast me parimin e përcaktimit me saktësi dhe korrektësi të normës penale. Ndaj, lypet nevoja e miratimit të një norme penale të posaçme/ad hoc për të ndëshkuar si sjellje më vete ato që kryhen nga përndjekësi me anë të përdorimit të mjeteve të teknologjisë.

Edhe pse **ligjvënësi danez** ([35]) ka meritën e adoptimit për herë të parë, që prej vitit 1933 me ndryshimet e vitit 1996 dhe 2004, të një norme penale *ad hoc* mbi *stalking,* ende sot që shkruajmë nuk ka një parashikim të shprehur në lidhje me fenomenin e *cyberstalking.* Kështu, sipas nenit 265 të kodit penal titulluar *"Forfolgelse",* përndjekje e vazhdueshme, integron elementët e kësaj vepre penale *"çdo veprim i autorit që cënon qetësinë e personit, e përndjek ose e shqetëson atë me veprime të përsëritura dhe invazive në sferën personale të tij "*. Dënimi në këtë rast është me burg deri në dy vite ose me gjobë.

Një veçori paraqet edhe qëndrimi i mbajtur nga **ligjvënësi irlandez**, i

34 Po aty.

35 Shih në faqen e internetit, file:///C:/Users/HP%20Pavilion/Documents/33156168.pdf aksesuar për herë të fundit më datë 10.8.2022.

cili që në vitin 1997 miratoi veprën penale të "*Non fatal Offences Aganist the Person Act*" – *Harrasment,* pra të sjelljeve përndjekëse. Në nenin 10 parashikohet: "*Cilido, që në mënyrë të vullnetshme ose jo, me sjellje ngacmuese, ndërhyn në jetën private të një personi, apo i shkakton frikë, ankth dhe dëme, me anë të përndjekjes së vazhdueshme, persekutimit apo komunikimit*, *dënohet me burgim gjer në shtatë vite ose me gjobë deri në 1.905 euro*"([36]). Edhe në këtë rast, ligjvënësi nuk ka parashikuar një numër të caktuar të këtyre veprimeve përndjekëse, por nisur nga togëfjalëshi *"në mënyrë persistente/të vazhdueshme"* nënkupton që vepra e *stalking* quhet e kryer kur ka patur të paktën një sjellje ngacmuese të përsëritur në kohë.

Po në të njëjtin vit, edhe **ligjvnësi anglez**([37])miraton "*Protection from Harassment Act*.", i cili parashikon *"Harassment" – ngacmime (art. 1)* dhe *"Putting people in fear of violence"* – sjellje, edhe pse verbale, që frikëson apo sjell ankth (art.4). Në këtë kuptim, që të jemi para kësaj vepre penale duhet të verifikohen të paktën dy episode ngacmimi, të cilat duhet të jenë të tilla që të frikësojnë apo shkaktojnë tek viktima gjendje ankthi. Dënimi është me burg gjer në gjashtë muaj ose gjobë deri në pesëmijë stërlina, apo të dyja së bashku.. Norma parashikon arrest të menjëhershëm në rastet kur janë të pranishëm të dyja kriteret *"Harassment"* dhe *"Putting people in fear of violence"([38]).* Megjithatë, edhe ligjvënësi i Mbretërisë Bashkuar, ashtu sikurse ai skocez, belg apo danez, nuk ka parashikuar një normë *ad hoc* apo rrethanë rënduese për veprimet përndjekëse të *cyberstalker*. Kështu, përndjekja nëpërmjet internetit nuk është një shkelje specifike sipas legjislacionit të Mbretërisë së Bashkuar, por mbulohet nga ligje të ndryshme (*përfshirë Ligjin për Mbrojtjen nga Ngacmimet 1997, Aktin e Krimeve Seksuale 2003 dhe Aktin e Barazisë 2010*). Ligji për Mbrojtjen nga Ngacmimet (1997) (PfHA) dhe Akti i Mbrojtjes së Lirive (2012) (PoFA) mund të përdoren për të ndëshkuar penalisht përndjekësit në Mbretërinë e Bashkuar. Edhe pse mjaft i gjerë për të lejuar ndjekjen penale të autorëve të përndjekjes kibernetike, Ligji për Mbrojtjen nga Ngacmimet nuk përcakton/ përkufizon përndjekjen kibernetike, gjë që rezulton në paqartësi në zbatimin në praktikë*(Bocij, Griffiths & McFarlane, 2002).* Për të adresuar këtë problematikë, disa sjellje tipike të cyberstalking janë përcaktuar në Aktin e Mbrojtjes së Lirive, përfshirë monitorimin nëpërmjet internetit, publikimin e materialeve për dikë tjetër dhe vjedhjen e identitetit. Ndërkohë që asnjëri

36 Shih "*Lo stalking*": *Comparazione tra le diverse esperienze giuridiche*, a cura di V. Iorio, Pegaso, Universita' telematica.

37 Po aty.

38 Shih në faqen e internetit, file:///C:/Users/HP%20Pavilion/Documents/33156168.pdf aksesuar për herë të fundit më datë 10.8.2022.

prej këtyre ligjeve nuk ofron mbrojtje kundër autorëve të paidentifikueshëm ose atyre që jetojnë jashtë Mbretërisë së Bashkuar **(***Salter & Bryden, 2009***)** ([39]).

Ndryshe nga legjislacionet evropiane, **Shtetet e Bashkuara të Amerikës** janë përpjekur të rregullojnë në mënyrë sistematike, që nga fundi i viteve '80 dhe fillimi i viteve '90, fenomenin e përhapjes së ngacmimeve, urrejtjes, dhunës verbale dhe bullizmit, me anë të përdorimit të mjeteve elektronike. Kështu, me Ligjin federal të vitit 1994 miratohej "*Violent Crime Control and Law Enforcment Act",* më anë të të cilit i jepej zgjidhje problemit të dhunës kundër grave, përfshirë këtu edhe keqtrajtimet dhe dhunën që ushtrohej ndaj tyre në ambientet e shtëpisë, ngacmimeve dhe agresioneve seksuale. Më tej, në vitin 1996, miratohet *"Interstate Stalking Punishment and Prevention Act".* Pra, veprës penale të *stalking* i jepej një formulim specific dhe me karakter detyrues edhe për shtetet e tjera amerikane. Po ashtu, gjithmonë në kuadrin e ligjeve federale, në vitin 2000 Kongresi amerikan miratoi "*Violence Againist Women Act (VAWA*) që ndëshkon përdorimin e postës elektronike apo të cdo lloji mjeti tjetër komunikimi, ndërmjet shteteve apo jashtë tyre, që kanë për qëllim ngacmimin apo përndjekjen e viktimës apo të pjestarëve të familjes së saj([40]). Po ashtu, shumë shtete amerikane kanë miratuar dispozita penale *ad hoc* për të rregulluar fenomenin *e "cyberstalking*" apo "*cyberharassment*". Kështu, me anë të "*Revised Code of Washington*" në vitin 2004, jepet shprehimisht një përkufizim i "*cyberstalkin*g". Ajo që vihet re në këtë përkufizim është dallimi që i bëhet *stalking* të thjeshtë nga *cyberstalking*, ku ligjvënësi përdor togëfjalëshin "*..and under circumstances not constituting telephone harassment, makes an electronic communication to such other person or a third party*"([41]). Pra, nga njëra anë, ligjvënësi përjashton nga *cyberstalking* të gjitha komunikimet telefonike, dhe nga ana tjetër, jep një përkufizim të qartë se çfarë do të kuptohet me komunikim elektronik për efekt të zbatimit të krimit të *cyberstalking*. Një përkufizim i tillë nuk është shumë bindës. Telefonata, vërtet është një mjet ideal në dorën e përndjekësit për të kryer një ngacmim/stalking ndaj viktimës, por nga ana tjetër, ndodhur tashmë para një epoke moderne dhe në prani të rrjeteve të ndryshme të telefonisë dixhitale, në veçanti "*Voice over IP (psh. software skype*), bërja e një diference mes telefonisë tradicionale dhe asaj dixhitale

39 Shih faqen e interentit, https://www.choose.co.uk/guide/online-harassment-cyberstalking-help.html aksesuar për herë të fundit më datë 10.8.2022.

40 Shih në faqen e internetit, https://cyber.harvard.edu/vaw00/cyberstalking_laws.html aksesuar për herë të fundit më datë 11.8.2022.

41 Shih G. Ziccardi në " *Cyberstalking and electronic devices: relevant legal-informatics issues",* Rassegna italiana di Criminologia, Anno VI N.3, 2012, fq. 165.

do të ishte e pavend dhe jo në hapat e kohës. Që do të thotë, se edhe me një komunikim telefonik autori mund të kryejë patjetër veprime tipike të *cyberstalking.* Përkufizime më pak të përgjithshme*, të cyberstalking,* jepen edhe në shtete të tjera si Florida, Utah, Virxhinia, South Dakota, Ohio, North Carolina etj., të cilat për shkak të volumit minimal të këtij punimi shkencor nuk mund të trajtohen([42]).

4. Praktika gjyqësore

Cyberstalking, sikurse u shpjegua edhe më lart, është një fenomen i ri i cili, sipas studiuesve, është gjithmonë në rritje. Kjo, për shkak edhe të evoluvimit të teknologjisë informatike dhe dixhitale, dhe lehtësirave që këto mjete i japin përdoruesit të tyre për të realizuar qëllimet kriminale. Për të rregulluar këtë fenomen, ligjvënësit kanë parashikuar në sistemet e tyre norma penale të posaçme ose, janë referuar në norma të tjera ekzistuese. Kjo ka bërë që edhe praktika gjyqësore, e secilit shtet, të trajtojë në mënyra të ndryshme rastet e përndjekjes informatike dhe dixhitale.

Gjykatat shqiptare, përpara miratimit të veprës penale të "*Përndjekjes*", përcaktuar në nenin 121/a të Kodit, këto veprime apo të tjera të ngjashme me to, sikurse u tha, i sanksiononin duke u referuar në vepra të tjera dhe të ndryshme penale([43]). Me miratimin e ligjit n. 23/2012 dhe parashikimin e posacëm të veprës penale të "*Përndjekjes*", gjykata është e kushtëzuar të vlerësojë faktet e ndodhura sipas përcaktimeve të kësaj dispozite. E mira materiale që kërkohet të merret në mbrojte nga norma penale është, përpos lirisë morale të individit kuptuar si e drejta për të vetëvendosur, edhe mbrojtja e sigurisë dhe shëndetit individual të viktimës, duke qënë se aktet e përndjekësit kanë mbi viktimën një efekt destabilizues në shëndetin, qëtësinë dhe ekuilibrin psikologjik të tij. Nga ana objektive, ky krim manifestohet me anë të veprimeve të një natyre të tillë të cilat në kontekstin e sjelljeve njerëzore janë të padëshirueshme, që shkaktojnë bezdisje, apo që çojnë në situata të pakëndshme. Kjo vepër karakterizohet nga sjellje alternative dhe nga fakte

42 Për një lexim më të thelluar,shih G. Ziccardi, op. cit., fq. 165 e vijues.

43 Si ajo e "*Kanosjes*" parashikuar në nenin 84; "*Plagosje e rëndë", " Plagosje e lehtë"* dhe *"Dëmtime të tjera me dashje"* parashikuar në nenet 88, 89 dhe 90, nëse për shkak të këtyre veprimeve me dashje të autorit viktimës i shkaktohej frikë, ankth e stres (tipike të kanosjes), apo pësonte një dëmtim, të rëndë apo të lehtë, në shëndetin e saj; "*Përhapja e sekreteve private*" parashikuar në nenin 122 – ku autori përhap me dashje një sekret të jetës private të një personi tjetër; "*Prishje e qetësisë publike*" parashikuar në nenin 274 - ku integron elementët e kësaj vepre penale edhe çdo lloj sjellje tjetër e papëlqyeshme e kryer në rrugë, sheshe a mjedise publike, që cënon dukshëm qetësinë e moralin e personit, dhe "*Përdorimi me keqdashje i thirrjeve telefonike*" parashikuar në nenin 275 - që bëhen me dashje nga autori për të prishur qetësinë e tjetrit.

jo të njëjta, por të ngjashme. Veprimet kërcënuese ose ngacmuese mund të jenë verbale ose fizike dhe mund të bëhen veçmas ose të kombinohen. Për shkak të këtyre sjelljeve viktima ndihet e frikësuar, përjeton ankth dhe tension të cilat bëhen pengesë për të jetuar normalisht jetën e saj.

Bazuar në këto elementë të veprës penale, Gjykata e Rrethit Gjyqësor Tiranë ([44]) do të shpallte fajtore shtetasen F.B., për kryerjen e veprës penale të ***"****Përndjekja",* parashikuar nga neni 121/a të Kodit Penal dhe dënimin e saj me 9 (nëntë) muaj burgim. Në gjykim rezultoi e provuar se e pandehura për një kohë gati një vjeçare përndiqte shtetasin L.Z. dhe bashkëshorten e tij E.Z. Në deklarimet e dhëna, e pandehura pranonte se e ka ndjekur vazhdimisht viktimën por, justifikohej me faktin se, këtë e ka bërë për shkak të ndjenjës dashurore që ka për shtetasin L.Z., të cilit ia ka shprehur në një rast duke i thënë *" unë ty të dua*". Edhe nga provat e tjera, vërtetohej që e pandehura ka përndjekur vazhdimisht këto dy shtetas, së bashku apo veç e veç, në ambiente të ndryshme si dyqane, shtëpi, lokale etj. Madje, në episode të caktuara ajo ka qenë afër me viktimat dhe aty i ka ngulur sytë shtetasit L.Z., duke i buzëqeshur dhe parë me inat bashkëshorten e tij E. Z., të cilën e ka kërcënuar me fjalët "*unë ty po të përcjell".* Për gjykatën e pandehura e ka kryer veprën penale për të cilën akuzohet[45].

Në vlerësimin e atij që shkruan, Gjykata në çështjen konkrete, jo vetëm ka zbatuar drejt ligjin, por ajo në përputhje me formulimin e ligjit jep edhe një përkufizim të atyre veprimeve të cilat mund të konsiderohen si sjellje përndjekëse kur shprehet se: " *këto veprime mund të jenë si psh. krijimi i kontakteve vizive ose fizike të përsëritura, komunikime pa dëshirën e personit tjetër, kërcënime verbale ose shkrime ose një kombinim i sjelljeve të tilla, që shkaktojnë ankth ose frikë për sigurinë vetjake të viktimës".*

---

44 Shih vendimin me numër Akti 565, n. 420 datë 16.02.2017.

45 Në vendimin e dënimit gjykata arsyeton*: "Ligji penal nuk përcakton numrin e veprimeve kërcënuese ose ngacmuese, të nevojshme që te jemi përpara kësaj figure vepre penale. Gjykata vlerëson se* ***mjaftojnë edhe dy episode*** *të kërcënimit ose ngacmimit, me kushtin që këto akte të shkaktojnë një gjendje të vazhdueshme (që zgjat) ankthi dhe frike të tilla që e cenojnë zhvillimin normal të jetës së përditshme që bënë viktima. Veprime apo sjellje "përndjekëse" mund të jenë: krijimi i kontakteve vizive ose fizike të përsëritura, komunikime pa dëshirën e personit tjetër, kërcënime verbale ose shkrime ose një kombinim i sjelljeve të tilla, që shkaktojnë ankth ose frikë për sigurinë vetjake të viktimës. (Në të paktën dy raste.) Në teorinë e të drejtës penale, kjo klasifikohet si një figurë materiale pasi, për ekzistencën e saj është e domosdoshme ardhja e pasojave shoqërisht të rrezikshme. Për rastin konkret shprehet gjykata, veprimet e kryera nga e pandehura janë të tilla, pasi për shkak të tyre viktimat L.Z. dhe E. Z., ndihen të kërcënuar dhe në një gjendje ankthi dhe frike në masën që u ka ndryshuar mënyrën dhe cilësinë e të jetuarit. Gjendje të cilën ata e kanë denoncuar para organeve përkatëse".*

Në një rast tjetër, po kjo gjykatë ([46]) me trup tjetër gjykuese, shpallte fajtor shtetasin grek M.D., për kryerjen e veprës penale të "*Përndjekjes*" dhe dënimin e tij me 6 (gjashtë) muaj burgim. Në aplikim të nenit 406 të K.Pr. Penale, përfundimisht i pandehuri M. D. u dënua me 4 (katër) muaj burgim. Ky shtetas kishte përndjekur viktimën B.T., për një kohë të vazhdueshme. Njohja e tyre kishte ardhur nëpërmjet *Facebook*-ut. Pasi i pandehuri ishte takuar disa herë me viktimën, i kishte kërkuar të lidhej me të. Pasi viktima kishte refuzuar të krijonte një lidhje dhe vendosi të ndërpreriste komunikimin me këtë shtetas, ky i fundit ka filluar me veprimet përndjekëse. Këto veprime shfaqeshin në forma të ndryshme, konkretisht duke u paraqitur personalisht dhe në mënyrë të përsëritur në ambientet e frekuentuara nga viktima dhe duke ushtruar dhunë fizike dhe psikike ndaj saj, ashtu edhe me anë të komunikimit në platformën dixhitale Skype dhe *Facebook*. Gjithashtu, nga deklarimet e viktimës del se, i pandehuri kishte krijuar po ashtu një mjedis në *Facebook* ku publikonte fotot e viktimës duke ecur në rrugë. Foto të cilat i pandehuri i bënte vetë. Siç shihet, nga rrethanat e faktit të provuara në gjykim del se autori për të realizuar qëllimin e përndjekjes ka përdorur edhe mjete të teknologjisë informatike dhe dixhitale. Duke përdorur këto mjete, ai jo vetëm ngacmonte dhe kërcënonte viktimën por shpërndante në profilin e tij të *Facebook-ut* edhe fotografitë ku pasqyrohej viktima. Veprime këto, që integrojnë elementët tipik të *cyberstalking*. Megjithatë, për gjykatën këto veprime do të konsideroheshin si të përfshira në parashikimet e nenit 121/a të Kodit, duke e trajtuar çështjen si përndjekje klasike. Ky vendim i është nënshtruar kontrollit të gjykatave më të larta ([47]), të cilat në përfundim kanë vendosur lënien në fuqi të vendimit të ankimuar/rekursuar, duke e gjetur kështu të drejtë cilësimin e veprës penale në raport me faktet e ndodhura.

Nga mënyra si janë arsyetuar vendimet e mësipërme, në të trija shkallët e gjykimit, por edhe praktika që po ndiqet në vijim([48]), na çon në mendimin

46 Shih vendimin n. 1941, datë 29.07.2014 të Gjykatës së Rrethit Gjyqësor Tiranë.

47 Shih vendimet e Gjykatës së Apelit Tiranë n. 784, datë 15.04.2015 dhe vendimit n. 241 28.12.2016 të Gjykatës së Lartë.

48 Një mori ëështjesh aktualisht janë në fazën e hetimeve apo gjykimeve, ku autorët ndiqen dhe dënohen sipas parashikimeve të nenit 121/a të K.penal, edhe pse veprimet e kryera prej tyre kanë ardhur kryesisht me përdorimin e mjeteve të teknologjisë, informatike dhe dixhitale. Kështu shtetasja L.S., pasi ishte goditur me biçikletë nga një shtetas, ky i fundit kishte filluar ta përndiqte atë duke i dërguar mesazhe ofenduese dhe kërcënime të përsëritura. Këto veprime ai i kryente me anë të internetit duke krijuar profile false në shumë adresa të Instagramit dhe Facebook. Çështja është në hetim dhe autori po ndiqet për veprën penale të parashikuar në nenin 121/a. Në një tjetër rast, ka nisur procedimi ndaj shtetasit B.R., i cili në mënyrë të përsëritur kishte ngacmuar dhe përndjekur viktimën edhe me anë të mjeteve informatike dhe dixhitale. Ky shtetas po ndiqet për veprën penale të parashikuar në nenin 121/a edhe pse veprimet e tij hyjnë në kategorinë e veprimeve tipike të *cyberstalking*. Gjykata e Apelit Tiranë me vendimin e saj

se për gjykatat tona nuk ka asnjë dallim midis përndjekjes klasike, për të cilin flet neni 121/a, dhe përndjekjes së kryer nëpërmjet përdorimit të mjeteve informatike apo dixhitale. Ndoshta, shtyrë nga mënyra e formulimit të dispozitës ku ligjvënësi ka përdorur tofjalëshat "*Kërcënimi ose ngacmimi i personit* ***me anën e veprimeve***". Dhe në kategorinë e "*veprimeve",* sipas gjykatës, përfshihet çdo lloj veprimi. Pra, edhe ato veprime përndjekjeje që kryhen me mjete të teknologjisë. Gjykojmë se një qëndrim i tillë do të shkonte përtej asaj që shprehimisht është përcaktuar në nenin 121/a. Nëse ligjvënësi do të kishte dashur që të përfshinte në kategorinë e veprimeve kërcënuese dhe ngacmuese edhe veprimet e kryera me anë të mjeteve informatike apo dixhitale, patjetër do t'a kishte shprehur një gjë të tillë. Mos zbatimi me korrektësi i ligjit nga ana e gjykatës, sipas frymës dhe gërmës së ligjit, çon në cënimin e parimit të taksativitetit. Gjykata në këtë mënyrë merr kompetencat e ligjvënësit, të cilat në rendin tonë kushtetues nuk i njihen.

Po ashtu, në rastet e trajtuara më lart vihet në dukje fakti se, gjykata nuk ka zbatuar masën e shtrëngimit personal të "*Arrestit me burg*", ndonëse pranon që vepra penale e "*Përndjekje*s" paraqet rrezikshmëri të lartë shoqërore, nisur nga masa e dënimit të lartë të parashikuar dhe përhapja shumë e gjerë e këtij fenomeni në komunitetin tonë. Këtë qëndrim ka mbajtur edhe Gjykata e Lartë në një rast ku thirrej për të vlerësuar kushtet e vendosjes së masës së sigurimit personal të dhënë ndaj përndjekësit, L.P, i cili sipas provave të mbledhura deri në atë moment të hetimit, kishte kërcënuar se do të vriste ish - bashkëshorten e tij nëse ajo nuk do të kthehej sërish me të. Në përfundim kjo gjykatë([49]) dispononte me prishjen e vendimit nr.469, datë 31.03.2016, të Gjykatës së Apelit Tiranë dhe lënien në fuqi të vendimit nr. 451 Akti, datë 21.02.2016 të Gjykatës së Rrethit Gjyqësor Tiranë, duke urdhëruar edhe lirimin e menjëhershëm të personit nën hetim L.P., ndaj të cilit ishte zbatuar masa e arrestit në burg.

Probleme jo të pakta, sa i takon kualfikimit të sjelljeve përndjekëse, ka hasur edhe jurisprudenca italiane. Kjo për shkak se, sikurse u tha edhe më sipër, përpara vitit 2009 në legjislacionin italian mungonte një normë penale

---

të datës 25.4.2019 la në fuqi vendimin e Gjykatës së Shkallës së parë Tiranë, që kishte caktuar ndaj personit nën hetim masën e sigurimit personal "*Arrest me burg"*.Në një rast tjetër, shtetasja L. V., përndiqej sistematikisht nga shtetasi B.L.. Përndjekja zgjati gati një vit. Ky shtetas në mënyrë të pësëritur i dërgonte lule viktimës, mesazhe me foto në celular, e kontaktonte nëpër rrjete sociale, tentonte ta takonte, në pikën sa ishte përplasur me grushte edhe me të dashurin e viktimës i cili kishte hyrë për të mbrojtur viktimën. Në përfundim gjykata vendosi dënimin e të pandehurit B.L., për veprën penale të "Përndjekjes" edhe pse tërësia e veprimeve të të pandehurit karakterizohej nga përdorimi i mjeteve informatike për të realizuar qëllimet e tij.

49 Shih vendimi n. 102 datë 18.05.2016.

ad hoc që sanksionone *stalking*. Ndaj për t'ju përgjigjur penalisht këtyre sjelljeve, gjykata italiane referohej tek dispozita të tjera penale si "*Molestia",* "*Minaccia"* dhe "*Maltrattamenti in famiglia*" parashikuar në nenet 660, 612 dhe 572 të Kodit penal. Mirëpo psh., në parashikimet e nenit 660 "*Molestie*"., hyjnë ngacmimet telefonike, edhe nëpërmjet sms, por jo veprimet e një *stalker* i cili përdor postën elektronike duke dërguar e-mail tek viktima. Ky veprim nuk sjell një ndërhyrje të menjëhershme në sferën e jetës private të personit që i drejtohet, pasi norma penale "*Molestie*" kërkon praninë e elementeve të tjera si vendi publik dhe përdorimi i telefonit. Ndaj kjo mënyrë të interpretuari dhe spostuari të qëllimit të normës penale, në mbrojtje të një të mire materiale të caktuar, binte ndesh me vetë nenin 25/2 të Kushtetutës dhe me nenin 1 të Kodit penal. Arsye përse, ligjvënësi italian në vitin 2009 formulon nenin 612-bis të Kodit penal titulluar "*Atti persecutori"*([50]).

Në formulimin origjinal, ligjvënësi nuk parashikonte rastet e përndjekjes së viktimës me anë të përdorimit të teknologjisë *(cyberstalking*) ndonëse ky fenomen ishte tashmë i njohur në praktikë. Edhe këtë rast, kjo harresë apo pakujdesi e ligjvënësit do të çonte gjykatën që të bënte sërish interpretime të zgjeruara të normës([51]) duke ndëshkuar penalisht, po me të njëjtën dispozitë të *stalking/atti persecutori,* edhe ato veprime përndjekëse të autorit të kryera me mjete informatike apo dixhitale([52]). Një praktikë e tillë kritikohej nga ana e doktinës, jo vetëm për shkak të interpretimit të s'forcuar që i bëhej dispozitës, duke cënuar parimin e taksivitetit([53]), që kërkon që gjykata t'i

50 Shih "*Cyberstalking; ne nuove frontiere del diritto penale"* në faqen e internetit https://www.diritto.it/cyberstalking-le-nuove-frontiere-del-diritto-penale/ aksesuar për herë të fundit më datë 11.8.2022.

51 Shih në faqen e internetit https://www.altalex.com/documents/neës/2010/09/08/stalking-su-facebook-l-invio-di-messaggi-e-video-hot-puo-essere-punibile aksesuar për herë të fundit më datë 11.8.2022. Në vendimin n. 32404 datë 16.8.2010, Gjykata e Cassacionit shqyrtonte rastin e një të dënuari i cili pasi kishte përfunduar një lidhje dashurore me viktimën, kishte filluar duke dërguar, me anë të facebook, video, mesazhe dhe foto që pasqyronte një raport intim të tyre. Këto materiale ia kishte dërguar edhe të dashurit të ex-it të tij. Edhe në këtë rast, për gjykatën këto veprime ngacmuese dhe të përsëritura integrojnë elementet e veprës penale të stalking, edhe pse ato janë kryer me përdorimin e mjeteve të teknologjisë, informatike sië është Facebook.

52 Shih në faqen e internetit, https://www.altalex.com/documents/neës/2011/10/10/ingiurie-e-minacce-su-facebook-e-stalking aksesuar për herë të fundit më datë 11.8.2022. Gjykata e Cassacionit italian me vendimin e saj n. 25488 datë 24 qershor 2011, thirrej për të shqyrtuar rastin e një të pandehuri i cili, pas ndërprerjes së bashkëjetesës dërgonte tek viktima, në mënyrë të përsëritur, mesazhe me anë të rrjetit social Facebook ku e kërcënonte atë. Madje në disa okazione, ai ishte paraqitur personalisht në vendet e frekuentuara nga viktima dhe e kishte rrahur atë. Për gjykatën këto veprime janë tipike të një *stalker* dhe si të tilla të ndëshkueshme sipas nenit 612 bis të kodit penal.

53 Shih S. Moccia. La promessa non mantenuta. Ruolo e prospettive del principio di determintezza e tassivita nel sistema penale italiano, Edizioni scientifiche italiane – Napoli. 2001, fq 13.

përmbahet me korrektësi dhe rreptësi ligjit ashtu sic është formuluar nga ligjvnësi, por edhe trajtimit të barabartë të këtyre dy sjelljeve, të cilat për nga kuptimi, mënyra, pasojat që shkaktojnë dhe natyra janë të ndryshme. Kështu, me Dekret ligjin n. 93 datë 14 gusht 2013, konvertuar në ligj me aktin normativ n. 119 datë 15 tetor 2013, ndryshohet paragrafi 2 i nenit 612 bis duke parashikuar një ritje të dënimit në rastet kur sjelljet e autorit përndjekës kryhen nëpërmjet përdorimit të instrumentave informatikë apo telematikë.

Me ndryshimet e pësuara, për gjykatën është qartësuar, deri diku, tashmë fenomeni i *stalking* dhe *cyberstalking.* Shprehemi në këtë mënyrë pasi Gjykata e Kasacionit italian([54]) do të ndërhynte sërish edhe në vitin 2015 duke saktësuar (edhe një herë) që veprimet kriminale të realizuara me anë të mjeteve teknologjike, njësoj do të disiplinohen sipas përcaktimeve të veprës penale të *stalking/akte persekutuese*. Kurse në një tjetër vendim([55]) të vitit 2019, Gjykata e Kasacionit do të shprehej se, autori do të përgjigjet në vartësi të mjeteve të përdorura për realizimin e veprime persekutuese, të cilat nëse janë mjete të teknologjisë, ai do të ndëshkohet sipas paragrafit të dytë të nenit 612-bis, që përbën edhe një dënim të rënduar.

Megjithatë, shumë autorë janë të mendimit se ka ardhur koha([56]) që *cyberstalking* duhet të formulohet në një dispozitë *ad hoc*. Një formulim *ad hoc* i cyberstalking do t'i ofronte viktimës një mbrojte më efikase dhe të përshtatshme nga ajo që i garantohet nëpërmjet nenit 612-bis. Një qasje

54 Shih në faqen e internetit , https://www.corsopraticodidiritto.it/l/il-reato-di-cyberstalking/ aksesuar për herë të fundit më datë 11.8.2022. Edhe në këtë rast, Gjykata e Cassacionit thirret për të shqyrtuar çështjen e një shtetasi Italian i cili nuk pranonte përfundimin e një lidhje dashurore. Pas përfundimit të kësaj lidhje, ai krijonte adresa false në rrjetet sociale në emër të ish të dashurës së tij duke mbledhur rreth këtij profili shumë maniakë seksualë të cilët, duke patur të dhënat e viktimës nga ish i dashuri, e kontaktonin personalisht viktimën duke i shprehur interes për takime e raporte intime. Madje ish i dashuri, kërcënonte viktimën, se do t'a ndëshkonte rëndë nëse nuk kthehej në lidhje me të. Për gjykatën këto akte persekutuese janë stalking dhe si të tilla ato cilësohen dhe penalizohen sipas parashikimeve të nenit 612-bis.

55 Shih në faqen e internetit, https://www.doppiadifesa.it/wp-content/uploads/2019/02/Stalking-e-uso-di-WhatsApp-Cassazione-penale-sez.-V-sentenza-28.01.2019-n.-3989.pdf aksesuar për herë të fundit më datë 11.8.2022. Në vendimin **n. 3989 datë 28.1.2019 Gjykata e Cassacionit konfirmon se kur një** *stalker* **i dërgon viktimës mesazhe kërcënuese apo ngacmuese nga sistemi WhatsApp, do të gjejë zbatim paragrafi i dytë i nenit 612-bis, për shkak se fakti konsiderohet i kryer nëpërmjet përdorimit të mjeteve informatike.**

56 Nisur nga premisa që ligjvënësi Italian e ka bërë një hap të tillë që me ligjin n. 69/2019 titulluar *" Violenza domestica e di genere*" "*Codice Rosso*", ku ka miratuar veprën penale të titulluar "*Diffusione illecita di immagini o video sessualmente espliciti* " - *Revenge porn* " parashikuar në nenin 612-ter dhe atë të *"cyberbullying*" ardhur me ligjin n.71 datë 19 qershor 2017. Bazuar në të njëjtat konsiderata por edhe mbi faktin e një mbrojtje sa më adekuate dhe efikase të fenomenit të *cyberstalking,* gjykojmë se duhet vijuar me një rregullim ligjor *ad hoc* ndaj këtij fenomeni.

e tillë, duhet të jetë jo vetëm për ligjvënësin italian, por edhe për ligjvënësit e tjerë të shteteve anëtare të Bashkimit Evropian dhe shtetet firmëtare të Konventës Evropiane për të Drejtat e Njeriut, nisur nga qëndrimi i mbajtur së fundmi nga Gjykata Evropiane për të Drejtat e Njeriut.

Kjo gjykatë, është investuar për të shqyrtuar çështjen me numër ankimi 35283/14 ndërmjet, *Khadija Ismayilova kundër shtetit të Azerbajxhanit*. Sipas ankueses shteti i Azerbajxhanit, në vijim i paditur, nuk kishte marrë asnjë masë për pengimin e cënimit të sferës së jetës private dhe reputacionit të saj, të drejta këto të njohura në nenin 8 të Konventës. Në rastin konkret, një portal online, për të kritikuar ankuesen dhe mënyrën e saj të të vepruarit, publikonte një video me përmbajtje seksuale ku pasqyrohej ankuesja. Sipas shtetit të paditur, kjo sjellje nuk është e ndaluar pasi duke qënë shpërndarësi një portal, ky veprim përbën shprehje të lirisë së mendimit për interes të publikut dhe informim të tij. Gjykata, duke konfirmuar një qëndrim të saj të mëparshëm, aktgjykimi i datës 10 janar 2019, apelet nr. 65286/13 dhe 57270/14, shprehet se: "*në fakt, nëse nga njëra anë Konventa mbron informacionin e përgjegjshëm për çështje me interes publik, sigurisht në përputhje me etikën e gazetarisë, nga ana tjetër, nuk mund të ketë një interes publik legjitim për të shfrytëzuar shkeljen e privatësisë së një personi, për të kënaqur kureshtjen e një numri lexuesish duke tallur publikisht viktimën dhe duke i shkaktuar asaj dëme të mëtejshme*". Në përfundim, Gjykata Evropiane për të Drejtat e Njeriut me vendimin e saj të datës 7 maj 2020 gjen shkelje të nenit 8 të Konventës([57]). Ky vendim ka rëndësi të veçantë, sepse tregon qëndrimin e palëkundur të kësaj gjykate në mbrojtjen e të drejtës së *privacy* dhe reputacionit të personit, të cilat nuk mund të cënohen me asnjë veprim, e aq më pak me përdorimin e mjeteve të teknologjisë, informatike apo dixhitale, sic ka ndodhur për rastin objekt gjykimi.

Në një çështje tjetër të vitit 2020, n. 56867/15, **Kjølbro, Buturugă contro Roumanie,** Gjykata Evropiane për të Drejtat e Njeriut[58] me vendimin e datës 11 shkurt dënonte shtetin rumun për shkelje të neneve 3 (*ndalimi i trajtimit çnjerëzor dhe poshtërues)* dhe 8 *(respektimi i të drejtës së jetës private, që përfshin edhe atë të privacy dhe korrespondencën)* të Konventës. Ankuesja u ishte drejtuar organeve vendase me një denoncim ndaj bashkëshortit të saj, duke pretenduar dhunë familjare të përsëritur, ndërhyrje abuzive në account/llogarinë e saj, përfshirë atë të Facebook,

57 Shih në faqen e internetit,https://globalfreedomofexpression.columbia.edu/cases/the-case-of-khadija-ismayilova-v-azerbaijan-no-3/ aksesuar për herë të fundit më datë 11.8.2022.

58 Shih në faqen e internetit, https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6910029-9279612%22]} aksesuar për herë të fundit më datë 12.8.2022.

hyrje në kompjuter duke përvetësuar dhe përdorur të dhënat personale dhe fotografi të saja si dhe përndjekje me anë të këtyre pajisjeve elektronike dhe dixhitale nga ana e ish bashkëshortit. Organi i ndjekjes penale kishte vendosur arkivimin (mos fillimin) e denoncimit duke i konsideruar veprimet e ish bashkëshortit jo si të rënda. Ky vendim ishte ankimuar nga viktima, dhe gjykata e shkallës së parë kishte disponuar me marrjen në mbrojtje për një periudhë 6 mujore, e cila gjithsesi nuk ishte zbatuar në mënyrë efektive. Për gjykatën, rastet e dhunës familjare duhet të trajtohen në mënyrë të ndryshme nga format e tjera të dhunës. Kjo, në harmoni me Konventën e Këshillit të Evropës "*Mbi parandalimin dhe luftën kundër dhunës së grave dhe asaj në familje"*, aprovuar në Stamboll më 11 maj 2011. Po ashtu, gjykata thekson se, *cyberviolence* njihet edhe në nivel ndërkombëtar si një " *figurë dhune kundër grave*", sic rezulton edhe në raportin e Organizatës së Kombeve të Bashkuara të vitit 2015 "*Cyberviolence kundër grave"* apo edhe në dokumentin e Grupit të Punës së Këshillit të Evropës të vitit 2018 *"Mbi stalking në web dhe forma të tjera të dhunës"*. Në vlerësimin e gjykatës, autoritet vendase nuk kanë marrë në konsideratë impaktin psikik që shkakon tek viktima kjo lloj dhune dhe as sensin e izolimit, të cilat shtyjnë viktimën shpesh herë drejt tërheqjes së denoncimeve. Për gjykatën, ka shkelje të Konventës edhe në rast se në shtetin e paditur ka një kuadër normativ të përshtatshëm dhe janë marrë urdhëra mbrojtje, por nuk është garantuar zbatimi efektiv i këtyre urdhërave([59]). Së fundmi, gjykata e sheh me rëndësi të madhe të theksojë se, *cyberviolence* duhet të konsiderohet si një formë dhune ndaj grave, e për rrjedhojë, autoritet kombëtare nuk mund të trajtojnë rastet e përdorimit abuziv të *account* të viktimës, përvetësimin ose përdorimin pa pëlqim të imazheve dhe të dhënave të viktimës nga ish bashkëshorti, si raste të një dhune të zakonshme([60]).

59 Shih në këtë drejtim edhe vendimin tjetër të GJEDNJ-së n. 41261/17, në cështjen *Volodina c. Russia, në faqen e internetit* https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-180628%22]} aksesuar për herë të fundit më datë 12.8.2022. Edhe në këtë vendim kjo gjykatë ka gjetur shkelje të nenit nenit 3 *(ndalimit të torturës*) dhe të nenit 3 në kombinim me nenin 14 të Konventës *(ndalimi i diskriminimit),* pasi viktima ankuese kishte pësuar nga ish partneri i saj dhunë sistematike në familje, kërcënime, goditje trupore që kishin shkaktuar abortin, vjedhje, publikim online pa pëlqimin e saj të fotografive private dhe instalimin të paisjeve gjurmuese GPS. Për gjykatën autoritet ruse kanë treguar neglizhence në mbrojtjen e këtyre të drejtave, në pikën që kanë shtyre viktimën të ndryshonte edhe gjeneralitet e saj për të mos u gjetur nga ish partneri.

60 Shih në faqen e internetit, http://www.marinacastellaneta.it/blog/cyberviolenza-contro-le-donne-interviene-la-cedu-cyber-violence-against-women-new-judgment-of-the-echr.html aksesuar për herë të fundit më datë 12.8.2022.

5. Konkluzione

Në përfundim të këtij hulumtimi, edhe pse jo shterues në tematikat e trajtuara, mund të arrihet në disa konkluzione që meritojnë të merren në konsideratë.

Së pari, të gjithë jemi të vetëdijshëm që teknologjia, informatike dhe ajo dixhitale, në dhjetë vjeçarin e fundit po njeh rritje të zhvillimit dhe përhapjes së saj. Interneti po përdoret masivisht nga ana jonë, si në ambientet familjare, ambientet e studimit, të punës por edhe të dëfrimit.

Së dyti, siç rezultoi nga analiza e kryer, fantazia dhe magjia e rrjeteve sociale, lehtësirat e krijuara në komunikim, ndërveprim dhe mundësia për të mbetur anonim, rrisin obsesionin e një individi për të keqpërdorur këto mjete dhe krijuar situata të rrezikshme përndjekje në dëm të personave të tjerë. Sipas studimeve të treguara, kuptuam që përndjekja me anë të mjeteve të teknologjisë është gjithmonë në rritje dhe ka efekte shkatërruese tek viktima e cila ndihet në ankth, e frikësuar dhe në gjendje të rënduar psikike, që mund të çojë, siç u tha, edhe në vetëvrasësje.

Së treti, detyra e çdo ligjvnësi përpara një fenomeni kaq të rrezikshëm dhe të këtyre përmasave, është ajo ndërgjegjësimit dhe ndërhyrjes së menjehershme duke formuluar normë penale *ad hoc* për mbrojtjen në mënyrë sa më efektive dhe të plotë të të drejtave të viktimës. Por rezultoi, se asnjë vend i Bashkimit Evropian, ndryshe nga sa është parashikuar në disa shtete të Amerikës, nuk ka parashikuar një normë penale *ad hoc* për të luftuar fenomenin e *cybertalking.* Sjelljet e *cyberstalker* vazhdojnë të ndështkohen me anë të dispozitave të *stalking.* Madje, në disa prej këtyre shteteve nuk ka të parashikuar as vepër penale të s*talking*, duke ndështkuar këto veprime me anë të dispozitave të tjera penale. Pra, veprimet përndjekëse, ngacmuese apo kërcënuese të *cyberstalker* edhe sot që shkruajmë konsiderohen njëjtë si *stalker,* pra si dhunë e zakonshme.

Së katërti, vendet e Bashkimit Evropian, por edhe shtetet e tjera të cilat rezultojnë firmëtarë të Konventave të këtij bashkimi, kanë detyrimin e respektimit të vendimeve të marra nga Gjykata Evropiane për të Drejtat e Njeriut, nëpërmjet zbatimit dhe uniformitetit të normativave përkatëse me jurisprudencën e krijuar nga kjo gjykatë. GJEDNJ-ja në çështjen e vitit 2020 n. 56867/15, mes **Kjølbro, Buturugă contro Roumanie**, ka theksuar se: ”*cyberviolence duhet të konsiderohet si një formë dhune ndaj grave, e për rrjedhojë, autoritet kombëtare nuk mund të trajtojnë rastet e përdorimit abuziv të account të viktimës, përvetësimin ose përdorimin pa pëlqim të imazheve dhe të dhënave të viktimës nga ish bashkëshorti,* ***si raste të një dhune të zakonshme****”.* Nëse kjo është e vërtetë, atëherë do të thotë se *cyberstalking,* nuk është dhe nuk duhet të trajtohet si një rast i akteve të zakonshme persekutuese, sic është *stalking.*

Së fundmi, nisur nga qëndrimi i GJEDNJ-së, por edhe dallimi thelbësor

që ekziston midis përndjekjes kibernetike me atë të përndjekjes klasike/ *stalking,* formulimi *ad hoc* i *cyberstalking* do të ishte një hap përpara në garantimin e një mbrojtje të plotë të viktimave.

Bibliografia

- De Fazio, L. dhe Sgarbi, C. "*Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno di cyberstalking"* , Rasagna Italiana di Criminologia anno VI. N.3. 2012.
- Di Maio, A. & La Muscatella, D. "*Il fenomeno di cyberstalking dopo la Novella legislative n. 119 del 2013: recenti questioni cocio-criminologiche ed attuali contrasti dogmatici",* Rasegna Italiana di Criminologia, Anno XII N. 1. 2018.
- Fiore, C. e Fiore, S. –"*Diritto penale"*, Pjesa e përgjithshme, casa edittrice Torino, anno 2008.
- Hamzaj, R. *Mes vlerave të traditës, meritës së ndryshimeve dhe largëpamësisë së ligjit dhe shoqërisë,* "*Keqinterpretimi dhe keqzbatimi i nenit 291 të K.Penal të Republikës së Shqipërisë, shkak i ndëshkueshmërisë pa ligj të shtetasve*" , Konferenca Shkencore Kombëtare, Drejtësia Penale Shqiptare
- Palazzo, F.C. "*Il pricipio di determintatezza nel diritto penale"*, CEDAM, Padova.
- Hamzaj, R "*Keqinterpretimi dhe keqzbatimi i nenit 291 të K.Penal të Republikës së Shqipërisë, shkak i dëshkueshmërisë pa ligj të shtetasve*".
- Av. Agim I. Tartari, Revista "*Avokatia*", nr.22.
- Mecani, D. e Drejta penale e posaçme.
- Padovani, T në, "*L'assenza di coerenza mette a rischio la tenuta del sistema"*, in *Guida diritto*, anno 2019.
- Romano, B. "*Diritto penale, Parte generale",* Terza edizione Giuffrè, Milano, 2016.
- Moccia, S. "*La promessa non mantenuta. Ruolo e prospettive del principio di determintezza e tassivita nel sistema penale italiano"*, Edizioni scientifiche italiane – Napoli. 2001.
- "*Lo stalking*": *Comparazione tra le diverse esperienze giuridiche*, a

cura di V. Iorio, Pegaso, Universita' telematica

- G. Ziccardi " *Cyberstalking and electronic devices: relevant legal-informatics issues",* Rassegna italiana di Criminologia, Anno VI N.3, 2012.
- "*Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno di cyberstalking*" në Rasegna Italiana di Criminologia, Anno. VI, Nr. 3. 2012.
- "*Countering Technologi-Facilitadet Abuse-Criminal Justice strategies for combating non consensual pornography, Sextortion, Doxing and Swatting*", RAND - 2020.
- Vendimi n. 16977 datë 4.6.2022 i Gjykatës së Cassacionit
- Vendimi n. 3989 datë 28.1.2019 i Gjykatës së Cassacionit
- Vendimi n. 32404 datë 16.8.2010 i Gjykatës së Cassacionit
- Vendimi n. 25488 datë 24.6.2011 i Gjykatës së Cassacionit
- Vendimi n. 420 datë 16.02.2017 i Gjykatës së Rrethit Gjyqësor Tiranë.
- Vendimi nr. 1941, datë 29.07.2014 i Gjykatës së Rrethit Gjyqësor Tiranë.
- Vendimi n. 784, datë 15.04.2015 i Gjykatës së Apelit Tiranë.
- Vendimi nr. 241 28.12.2016 i Gjykatës së Lartë.
- Vendimi n. 102 datë 18.05.2016 i Gjykatës së Lartë.
- Ligji n. 69/2019 titulluar *" Violenza domestica e di genere*" "*Codice Rosso*"
- Kodi Penal i Republikës së Shqipërisë
- Kodi Penal Italian

Vendimi i GJEDNJ-së n. 41261/17, në çështjen *Volodina c. Russia, në faqen e internetit* https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-180628%22]}

- Vendimi i GJEDNJ-së në çështjen me numër ankimi 35283/14 *Khadija Ismayilova kundër shtetit të Azerbajxhanit.*
- Vendimi i GJEDNJ-së në çështjen n. 56867/15 të vitit 2020, Kjølbro, Buturugă *contro Roumanie.*

Web:

"*Cyberstalking; ne nuove frontiere del diritto penale"* Url: https://www.diritto.it/cyberstalking-le-

nuove-frontiere-del-diritto-penale/

McFarlane&Bocij, https://www.unobravo.com/post/cyberstalking-relazioni-in-rete.

Anti-Defamation League, "*Online Hate and Harassment: The American Experience*" Url: https://www.adl.org/onlineharassment#survey-report

Gordon Sh. *"What is Cyberstalking?",* Url: https://www.verywellmind.com/what-is-cyberstalking-5181466

Eurispes, Rapporto Italia 2017. *L'87,5% dei giovanissimi è stato vittima di cyber stalking* Url: https://eurispes.eu/news/eurispes-rapporto-italia-2017-l875-dei-giovanissimi-e-stato-vittima-di-cyber-stalking/

Chi era Tiziana Cantone: tutta la storia e le ultime notizie Url: https://notizie.virgilio.it/tiziana-cantone-storia-ultime-notizie-1498093

Concas A. "*Il reato di revenge porn"* Url: https://www.diritto.it/il-reato-di-revenge-porn

"*Amanda Todd: Memorial for teenage cyberbullying victim*", Url: www.bbc.co.uk/newsbeat/article/19960162/amandatodd-memorial-for-teenage-cyberbullying-victim

Montini B. *"Si suicida dopo uno stupro , la sua foto finisce in una pubblicità su Facebook"*, url: https://www.corriere.it/esteri/13_settembre_18/facebook-usa-foto-ragazza-suicida-dopo-stupro-proteste-e-scuse_03f6e1bc-2067-11e3-8197-f40f962f8de4.shtml

Yandoli K.L. "*Revenge Porn's Latest Casualty",* Url: https://www.bustle.com/articles/9485-revenge-porn-legislation-called-for-in-brazil-following-17-year-olds-suicide

Sicuro P. "*Cyberstalking: le nuove frontiere del diritto penale*", Url: https://www.diritto.it/cyberstalking-le-nuove-frontiere-del-diritto-penale/

"Stalking e temporaneo riavvicinamento della vittima al persecutore" Cassazione penale, sez. V, sentenza 04.06.2020, n. 16977, Url: https://www.doppiadifesa.it/wp-content/uploads/2020/06/Stalking-e-riavvicinamento_Cassazione-penale-sez.-V-sentenza-04.06.2020-n.-16977.pdf,

Kukiewicz, J. "*Should broadband providers be tackling online harassment?*", Url: https://www.choose.co.uk/guide/online-harassment-cyberstalking-help.html

"*State and Federal Stalking Laws*", Url: https://cyber.harvard.edu/vaw00/cyberstalking_laws.html

Rinaldi M. "*Stalking su Facebook: l'invio di messaggi e video hot può essere punibile*", Url: https://www.altalex.com/documents/news/2010/09/08/stalking-su-facebook-l-invio-di-messaggi-e-video-hot-puo-essere-punibile

Giancristofaro A.A. "*il reato di cyberstalking in epoca moderna: tra*

normativa e giurisprudenza", Url: https://www.corsopraticodidiritto.it/l/il-reato-di-cyberstalking/

"*Cyberviolenza contro le donne: interviene la CEDU – Cyber violence against women: new judgment of the ECHR*", Url:http://www.marinacastellaneta.it/blog/cyberviolenza-contro-le-donne-interviene-la-cedu-cyber-violence-against-women-new-judgment-of-the-echr.html

"THE ROLE OF TECHNOLOGY IN PREVENTING AND COMBATING ORGANIZED CRIME, FINANTIAL CRIMES AND CORRUPTION-ABSTRACT SUBMISSION"

INTELLECTUAL PROPERTY RIGHTS AND LEGAL PROTECTION

DR. SAIMIR SHATKU

FVFR, UST - Tirana-Albania

s_shatku@yahoo.com

DR. MIMOZA SADUSHAJ

NCHN - Tirana-Albania

Abstract

In recent years, we can say that the whole world is in a constant revolution of using technology and disseminating information quickly and efficiently, eliminating previous barriers that existed between countries.

Digitalization is taking giant steps, in a world where distance is losing its effect and relationships are being concretized every time through the virtual and digital world.

Technology in this aspect plays its indisputable role, as with the perfection of its operation and methods, favorable conditions have been created for the creation and use of digital works.

But their use is not the same everywhere in the world, as in different

countries the use of digital works is considered different and does not always constitute a violation of copyright.

Every individual is capable of creating a digital work and exercising the basic rights deriving from it by also undertaking all actions for the free use and according to his desire of this work.

It is impossible in a digital environment, not to have creativity from many individuals, who in order to simplify lifestyles be influenced by taking various actions, which are related to their reproduction for profit or relief effects.

Often these ways of reproduction of these works are not realized according to the criteria set by the legislation, but create conditions for abuses, violating the rights of the real authors of these rights.

For this reason, the right to personal use of digital works is very important, in the virtual environment from which we are surrounded and in order not to create causes for abuse, it is necessary to get acquainted with the most important aspects that it addresses. In this regard, it is the duty of the state as a regulator, through concrete measures and reforms undertaken by it, to create conditions for the prevention of these violations and the regulation of concrete consequences to a large extent for the protection of intellectual property.

The right of competition, and the right of intellectual property, are two important rights for every individual in his affirmation, which often collide with each other thus creating conditions for unfair benefits and their violation by each other.

Key words: Intellectual property; legal protection; abuse; digitization; reproduction

E DREJTA E PRONËSISË INTELEKTUALE DHE MBROJTJA LIGJORE

Abstrakt

Vitet e fundit, mund të themi se e gjithë bota është në një revolucion të vazhdueshëm të përdorimit të tekonologjisë dhe shpërndarjes së informacionit në mënyrë të shpejtë dhe efikase, duke eleminuar barrierat e mëparshme që ekzistonin ndërmjet vendeve.

Dixhitalizimi po ecën me hapa gjigandë, në një botë ku largësia po e humb efektin e saj dhe marrëdhëniet po konkretizohen çdo herë nëpërmjet botës virtuale dhe dixhitale. Teknologjia në këtë aspekt luan rolin e saj të padiskutueshëm, pasi me përsosjen e funksionimit dhe metodave të saj, janë krijuar kushte favorizuese për krijimin dhe shfrytëzimin e veprave dixhitale. Ky shfryëzim dhe përdorim i tyre nuk është i njëjtë kudo në botë, pasi në vende të ndryshme përdorja e veprave dixhitale konsiderohet e ndryshme dhe jo gjithmonë përbën cenim të së drejtë së autorit.

Çdo individ është i aftë të krijojë një vepër dixhitale dhe të ushtrojë të drejtat kryesore që burojnë prej saj duke ndërmarrë gjithashtu të gjitha veprimet për përdorimin e lirë dhe sipas dëshirës së tij të kësaj vepre. Është e pamundur që në një mjedis dixhital, të mos të ketë krijimtari nga shumë individë, të cilët në mënyrë që të thjeshtëzojnë mënyrat e jetesës të ndikohen duke ndërmarrë veprime të ndryshme, të cilat lidhen me riprodhimin e tyre për efekte përfitimi ose lehtësimi.

Shpeshherë këto mënyra riprodhimi të këtye veprave, nuk realizohen sipas kritereve të përcaktuara nga legjislacioni, por krijojnë kushte për abuzime, duke cenuar të drejtat e autorëve real të këtyre të drejtave.

Për këtë arsye, e drejta për përdorim vetjak e veprave dixhitale, është shumë e rëndësishme, në mjedisin virtual nga i cili rrethohemi dhe në mënyrë që të mos krijojë shkaqe për abuzime, është e nevojshme që të njihemi me aspektet më të rëndësishme që ajo trajton.

E drejat e konkurrencës, dhe e drejta e pronësisë intelektuale, janë dy të drejta të rëndësishme për këdo individ në afirmimin e tij, që shpeshherë përplasen me njëra tjetrën duke krijuar në këtë mënyrë kushte për përfitime të padrejta dhe cënim të tyre nga njëri tjetri.

Në këtë aspekt, është detyrë e shtetit si rregullator, që nëpërmjet masave konkrete dhe reformave të ndërmarra nga ana e tij, të krijojë kushte për

parandalimin e këtyre shkeljeve dhe rregullimit të pasojave konkrete në një masë të gjerë për për mbrojtjen e produktit intelektual.

Fjalë kyçe: Pronësia intelektuale; mbrojtje ligjore; abuzim; digjitalizim; riprodhim

Mbrojtja e se drejtës së autorit

Autori i veprës është pronari i parë i të drejtave vetjake jopasurore dhe pasurore që janë të lidhura me veprën e tij. Po të analizojmë ligjin "Për të drejtën e Autorit" vihet re përcaktimi se e drejta e pronësisë mbi një vepër i jep të drejtë autorit apo pronarit të saj që të caktojë fatin e veprës, të kalojë të drejtën e pronësisë së veprës tek një person tjetër, ta tjetërsojë atë, ta shesë, ta importojë, ta japë me qera, etj. Në këtë ligj përcaktohet se autori është pronari i të drejtës së autorit, përcaktohet se autori është pronari i parë i veprës që ai ka krijuar, sepse pas tij mund të vijnë pronarë të tjerë, të cilëve u kalon e drejta e pronësisë mbi veprën në forma të ligjshme.

E drejta e autorit është e drejta eskluzive e dhënë nga autori i saj për kopjimin ose përdorjen e veprës së tij krijuese nga persona të tretë. Ajo lind automatikisht në momentin e krijimit të veprës origjinale ose të prejardhur dhe aplikohet në të gjitha veprat origjinale letrare, shkencore dhe artistike. E drejta e autorit dhe të drejtat e lidhura me të janë të drejta thelbësore për krijimtarinë njerëzore, duke u dhënë në këtë mënyrë nxitje krijuesve në formën e njohjes dhe shpërblimeve të drejta ekonomike.

Me pak fjalë, mund të themi se e drejta e autorit është mbrojtja ligjore e ofruar për titullarin e të drejtave që rrjedhin nga një vepër origjinale që ai ka krijuar. Në vitin 2005 në vendin tonë, u aprovua ligji "Për të drejtën e autorit dhe të drejtat e tjera fqinje të lidhura me të", i cili bëri një rregullim dhe mbrojtje më të plotë për këtë institut të së drejtës.

Legjislacioni i të drejtës së autorit është pjesë e një legjislacioni më të gjerë, i njohur ndryshme si pronësi intelektuale dhe që përfshin në vetvete mbrojtje të gjerë për çdolloj krijimi ose shpikje të një individi, duke i njohur atij të drejtën e pronës mbi krijimet.

Parimi i çdo lloj prone është që pronari mund ta përdorë atë ashtu siç ai dëshiron dhe që askush tjetër, nuk është i legjitimuar ta përdorë pa autorizimin e tij. Të drejtat e mbajtësit të së drejtës të një vepre të mbrojtur, të garantuara në ligjet kombëtare, janë normalisht të drejta ekskluzive, për të autorizuar një palë të tretë për të përdorur veprën, subjekt i të drejtave dhe interesave të ligjshëm të të tjerëve.

Qëllimi i të drejtave të lidhura me të drejtën e autorit është të mbrojë interesat ligjore të personave të caktuar dhe entiteve të legjitimuara, të cilët kontribuojnë për të vënë në dispozicion të publikut, veprat.

Gjatë periudhës së tranzicionit në Shqipëri, mund të themi se janë sanksionuar një sërë të drejtash të autorit dhe gjithashtu të pasojave të ardhura nga cenimi i tyre. Kjo shprehet më së miri në Kushtetutën e Republikës së Shqipërisë, e cila sanksionohet lirinë e krijimtarisë dhe garanton mbrojtjen e saj.

Ndryshime të rëndësishme janë bërë me hyrjen në fuqi të Kodit Penal dhe të Kodit Civil, të cilat në dispozitat e tyre e kanë trajtuar këtë insitut. Mbrojtja që ofrohet nga dispozitat e Kodit Penal[1], konkretisht në nenet 148 dhe 149, që lidhin kundravajtjen penale të botimit të veprës së tjetrit me emrin e vet dhe me riprodhimin pa të drejtë të veprës së tjetrit, parashikojnë padyshim një mbrojtje për këtë insitut të së drejtës.

Ndërsa, nga dispozitat e Kodit Civil[2], që kanë të bëjë me shkaktimin e dëmit jopasuror kundrejt emrit, personalitetit dhe veprës së një personi, apo me publikimet mashtruese të bëra nga subjekte që ushtrojnë aktivitetin e tyre në fushën e botimeve, del në pah raporti tjetër midis së drejtës së autorit dhe legjislacionit civil.

Pra, siç shihet edhe nga këto parashikime, e drejta morale dhe ekonomike e autorit, gëzon mbrojtjen e tyre ligjore, si një e drejtë mjaft e rëndësishme për shoqërinë në tërësi dhe për individin në vecanti.

Në kreun IX të ligjit "Për të drejtën e autorit", në nenin 50 përcaktohet se në rast shkeljesh të të drejtave të përcaktuara në këtë ligj, personat mund t`i drejtohen gjykatës, me anë të padisë civile ose me anë të denoncimit për ndjekje penale sipas dispozitave të Kodit Penal në organet përkatëse. Gjykata shqyrton çështjen në bazë të normave të përcaktuara në këtë ligj dhe në përfundim vendos si për të drejtat morale, ashtu dhe për ato ekonomike të autorit.

Legjislacioni dhe dispozitat e tij mbi pronësisë intelektuale në Shqipëri garantojë sigurimin e mbrojtjes së përshtatshme dhe efikase të zbatimit të drejtave të autorit në një nivel të njëjtë mbrojtjeje të të drejtave të pronësisë intelektuale me ato ekzistuese në Bashkimin Europian, si dhe garantimi i vazhdueshëm i harmonizimit të nivelit të mbrojtjes në përputhje me të gjitha

1 Kodi Penal i Republikës së Shqipërisë, 2017

2 Kodi Civil i Republikës së Shqipërisë, nenet 635 dhe 640. Kodi Civil 1929, Tiranë 2010, botimet Papirus, f. 279.

detyrimet ndërkombëtare dhe marrëveshjet që Republika e Shqipërisë është palë.

Për ta bërë më konkrete këtë cështje, le të analizojmë konkretisht disa nga pasojat ligjore që vijnë nga cenimi i së drejtës së autorit, të parashikuara konkretisht në Ligjin nr. 9380 datë 28.04.2005 "Për të drejtën e autorit dhe të drejtat e tjera të lidhura me të ". Ndërsa dispozitat e tjera parashikojnë:

Neni 31

"*Autori, veprat e të cilit, për shkak të natyrës mund të riprodhohen pa autorizim në kushtet e nenit 72 nëpërmjet fotokopjes, ...autorët kanë të drejtën e shpërblimit të arsyeshëm nga një person fizik ose juridik, i cili ofron shërbimet e fotokopjimit me pagesë".*

Një shpërblim i arsyeshem i referuar në këtë nen do të jetë ai shpërblim i dhënë me marrëveshje, duke marrë parasysh mundësinë e dëmit të shkaktuar autorit të veprës, në rastet kur vepra është riprodhuar pa autorizimin e tij për përdorim privat ose përdorime personale të tjera, aplikimin e masave teknologjike mbrojtëse, si dhe të rrethanave të tjera që mund të konsiderohen të drejta në formë dhe përmbajtje për një shpërblim të arsyeshëm.

Kur flasim për disa kufizime të së drejtës së autorit, do të kemi parasysh rastin kur vepra ose pjesë të saj mund të përdoren nga subjektet e interesuara pa marrë lejen paraprake të autorit. Këto raste kufizimesh janë taksative. Në raste të tjera duhet të bëhet shumë kujdes që përdorimi i veprës të jetë në mënyrë të drejtë. Në disa raste përdorimi i drejtë rregullohet me titull nga autori, në raste të tjera ai quhet i drejtë dhe nuk ka nevojë për një autorizim të posaçëm. Ligji parashikon kufizimet në ushtrimin e të drejtës së autorit dhe përdorimi i veprës pa lejen e autorit parashikon se: "Lejohet përdorimi i një vepre pa miratimin e autorit dhe pa asnjë shpërblim, me kusht që të mos cënohet e drejta e autorit ose e titullarit të të drejtës së autorit mbi veprën kur";

a) Gjatë riprodhimit të shkrimeve të veçanta a të pjesëve të shkëputura të veprës në botimet ditore, periodike ose në transmetimet radiotelevizive përmendet emri i autorit dhe burimi, ose kur është parashikuar shprehimisht ndryshe;

b) Gjatë riprodhimit të fjalimeve të mbajtura në tubime publike, të publikuaravnë botime ditore a në periodikë të ndryshëm apo të transmetuara për publikun në radio ose televizion, citohen, sëbashku me emrin e autorit, data dhe vendi i mbajtjes së fjalimit;

c) Riprodhimi i plotë ose i një pjese të saj në një procedurë gjyqësore apo administrative, por gjithnjë në masën e justifikuar nga qëllimi për të cilin përdoret dhe duke përmendur burimin e veprës dhe autorin e saj;

d) Riprodhimi i plotë ose i një pjese të saj bëhet për përdorim vetjak, me kusht që të mos cënojë shfrytëzimin tregtar të veprës;

e) Riprodhimi i veprës së fiksuar në një mbajtës zëri dhe/ose figure apo në një mbajtës grafik, bëhët nga një person fizik, për përdorim vetjak apo familjar, pa kryer asnjë veprim të drejtëpërdrejtë ose të tërthortë për qëllime tregtare;

f) Fotokopjimi i veprave të bibliotekave publike bëhet për përdorim vetjak brenda bibliotekës ose për shërbime të saj.

Por ç'farë nënkupton termi "përdorim vetjak"? Sipas autores Semini, termi përdorim vetjak sipas ligjit "Për të drejtën e autorit" nënkupton një përdorim të veprës në familje, si psh një riprodhim i një pikture, i një qilimi etj, apo përdorimi i tyre në ambjente personale. Këtu do të futet edhe përdorimi për qëllime pedagogjike, kërkimore, shkencore.

Për shkeljet e së drejtës së autorit, nëse nuk arrihet një marrëveshje midis palëve, personat e interesuar mund t'i drejtohen gjykatës që ta zgjidhë konfliktin në një gjykim civil.

Përveç zhvillimit të procesit civil, në kuadër të mbrojtjës së të drejtës së autorit, për vetë rëndësinë që ajo paraqet dhe pasojave që vijnë nga shkelja e saj, e drejta e autorit mbrohet edhe nëpërmjet zhvillimit të procesit penal.

Kodi Penal, në dispozitat e tij bën një parashikim të hollësisëhm të shkeljve të këtyre të drejtave ku konkretisht parashikohet:

Neni 149 i Kodit Penal parashikon se: - *"Riprodhimi tërësisht ose pjesërisht i veprës letrare, muzikore, artistike, ose shkencore që i përket një tjetri ose përdorimi i tyre pa pëlqimin e autorit, kur janë shkelur të drejtat vetjake e pasurore të tij, dënohet me gjobë ose me burgim deri në 2 vjet"*[3].

Ndërsa neni 148 i Kodit Penal i vjen në mbrojtje të drejtës morale të autorit për t'u njohur si autori i veprës së tij kur parashikon se: *"Botimi ose përdorimi tërësisht apo pjesërisht me emrin e vetë të një vepre letrare, muzikore, artistike ose shkencore, që i përket një tjetri, përbën kundravajtje penale dhe dënohet me gjobë ose me burgim gjer në 2 vjet"*.

Referuar në këto dispozita, vërejmë se legjilsacioni penal dhe civil i japin mbrojtje dhe trajtojnë pasojat që vijnë nga cënimi i të drejtave të autorit.

3 Kodi Penal i Republikës së Shqipërisë, ndryshuar 2017, neni 149.

Konkluzione

Nga ajo çka trajtuam më sipër në këtë punim, mund të themi se legjislacioni për të drejtën e autorit në vendin tonë, trajton aspekte të rëndësishme të mbrojtjes së tij duke parashikuar gjithashtu sanksione për këdo që i cenon ato. Ky legjislacion, është hartuar në përshtatje me dispozitat e legjislacionit ndërkombëtar për këtë qëllim, i cili duhet pranuar se i ka kushtuar një rëndësi të gjerë kësaj të drejte. Në këto kushte, Shqipëria ka ratifikuar dhe inkoporuar një sërë direktivash dhe konventash për afirmimin dhe mbrojtjen e mëtejshme të kësaj të drejte të gjerë, në mënyrë që të mbrojë këdo që cenohet padrejtësisht gjatë ushtrimit të të drejtave të tij të autorësisë.

Gjithësesi, mund të themi se mbetet ende shumë për të bërë dhe legjislacioni ka vend për përmirësime të mëtejshme, si dhe për rritjen e masës së dënimit dhe sanksonit, për këdo që cenon këto të drejta.

Referenca

- Kushtetuta e Republikës së Shqipërisë, 2017;
- Kodi Civil i Republikës së Shqipërisë, 2017;
- Kodi Penal i Republikës së Shqipërisë, 2017;
- Semini. M, “E drejta e autorit”, Scanderbeg books, Tiranë 2009;
- Koci. E, « Pronësia Intelektuale, E drejta e Autorit dhe Markat », Dhjetor 2003;
- Zajm.I, “E drejta e Bashkimit Europian – Historia e integrimit europian, institucionet, tregu i përbashkët”.
- F. Dega, “Pronësia intelektuale” botim i II i ripunuar, Tiranë, 2008;
- Semini M, “E drejta e detyrimeve dhe e kontratave”, Shtepia Botuese Afërdita, 2009;
- Konventa e Bernës « Për mbrojtien e veprave letrare dhe artistike » (1971);
- Konventa Universale për të Drejtën e Autorit;
- Ligji nr. 9380 datë 28.04.2005 “Për të drejtën e autorit dhe të drejtat e tjera të lidhura me të “.

KRIPTOMONEDHAT DHE PËRDORIMI I TYRE NË BOTËN KRIMINALE

MSC. INA VELESHNJA

Asistente Lektore, Departamenti Penal

Ina.veleshnja@fdut.edu.al;

INVA KOCIAJ

Asistente Lektore, Departamenti Civil

Inva.kociaj@fdut.edu.al

Abstrakt:

Zhvillimet teknologjike kanë ndikuar në jetën tonë të përditshme duke sjellë ndryshime rrënjësore jo vetëm në mënyrën e të jetuarit, të menduarit të vepruarit dhe ndërvepruarit me njëri tjetrin, por mbi të gjitha duke afruar gjithnjë e më shumë realen me virtualen. Vendi ynë si fundmi ka miratuar edhe ligjin nr.66/2020 "Për tregjet financiare të bazuara në teknologjinë e rregjistrave të shpërndarë", duke e renditur Shqipërinë në vendet e pakta në Europë që ka miratuar një ligj për njohjen e monedhave digjitale. Një person i panjohur krijoi kriptomonedhën e parë digjitale në botë të njohur me emrin "Bitcoin". Kjo monedhë digjitale mund të trasferohej peer-to-peer pa pasur nevojën e një insitucioni të centralizuar, i cili të mund të ndërhynte në proces. Kushti thelbësor është anonimati, ku askush nuk e di identitetin e palës tjetër me të cilën po bën transaksione online. Fatkeqësisht, ky element i anonimatit dhe fshehjes online po përdoret gjerësisht nga grupet kriminale të cilat përfitojnë për kryerjen e veprave penale të ndryshme. Në këtë punim

do të njihemi me një nga zhvillimet teknologjike në krijimin e monedhave digjitale, si u krijuan ato, përdorimi, shkëmbimi, efektet pozitive që kanë sjellë si dhe ato negative, dhe përvetësimi dhe përdorimi i tyre nga indvid apo organizata kriminale duke krijuar kësisoj, kushtet ideale për konsumimin e disa veprave penale.

Fjalët kyc: monedha digjitale, bitcoin, vepër penale, skema mashtrimi, krimi kibernetik, organizata kriminale

Hyrje

1. Si u krijuan kriptomonedhat?

Revolucioni i katërt në botë ndodhi pikërisht në teknologji. Zhvillimet teknologjike po ridimensionojnë jo vetëm konceptet tona për jetën, përditshmërinë, për individin, por vitet e fundit po na njohin me monedhën virtuale. Në fillimet e njerëzimit tregtia kishte si bazë shkëmbimin e mallit me mall, më pas të mallit me monedhën, sot po përballemi me një ndryshim të madh siç është përdorimi, përvetësimi i monedhës digjitale. Sot njeriu blen, shet, kryen transaksione nëpërmjet një monedhe të cilën nuk e prek asnjëherë por me të cilën mund të kryejë një sërë veprimesh në botën e pafundme të internetit.

Monedha e parë digjitale është Bitcoin, e krijuar në vitin 2008 dhe e formuluar mbi koncpetin e rrjetit "peer – to – peer" (P2P) [1]. Qëllimi i konceptit "peer – to – peer" (P2P) është kalimi i pagesave online në mënyrë të drejtpërdrejtë nga njëra palë te tjetra por duke shmangur institucionet financiare. Ajo u krijua nga një person i cili zgjodhi të quhej Satoshi Nakamto duke mbajtur anonim emrin e tij të vërtet [2]. Monedha digjitale bitcoin ka dy karakteristika së pari ajo është e decentralizuar, pra nuk i nënshtrohet asnjë kontrolli prej institucioneve finanaciare dhe së dyti ka karakter digjital, pra ajo nuk ka asnjë vlerë fizike siç kanë monedhat e argjendit apo të bakrit. Praktikisht nëse ne jemi mësuar që ti mbajmë paratë tona në xhep ose në portofol, bitcoin qëndron në kompjuter ti nuk e prek asnjëherë. Kjo monedhë është thjesht një kod alfanumerik i kriptuar pra i koduar të cilin është shumë i vështirë për t'u dëshifruar dhe e ruan në kompjuterin tënd.

Nakamato krijoi gjithashtu edhe bazën e të dhënave blockchain [3].

1 Kayal, P., Rohilla, P. Bitcoin in the economics and finance literature: a survey. *SN Bus Econ* **1,** 88 (2021). https://doi.org/10.1007/s43546-021-00090-5.

2 WIKIPEDIA https://en.wikipedia.org/wiki/Bitcoin

3 WIKIPEDIA https://en.wikipedia.org/wiki/Blockchain

Blockchain është një listë e të dhënave që rritet gjithë kohës dhe që quhen ndryshe blloqe, të gjitha këto të dhëna janë të lidhura së bashku në një mënyrë të sigurtë duke përdorur kriptografinë [4]. Teknologjia blockchain krahasohet lehtësisht me një libër të decentralizuar i cili rregjistron origjinën e një aktivi digjital, gjithashtu të dhënat nuk modifikohen duke e bërë blockchain një rrjet të sigurtë si për pagesat, sigurinë kibernetike por edhe për kujdesin shëndetësor. Blockchain konsiderohet të jetë një nga platformat më të mira dhe teknologjia më e sofistikuar që nga zbulimi i internetit. Bitcoin është ndërtuar në një regjistër transaksionesh që shpërndahen në një rrjet kompjuterash pjesëmarrës. Dizajni i Bitcoin lejon transaksione të pakthyeshme, një rrugë të përcaktuar të krijimit të parave me kalimin e kohës dhe një histori transaksionesh publike [5]. Çdokush mund të krijojë një llogari Bitcoin, pa pagesë dhe pa ndonjë procedurë të centralizuar verifikimi—ose edhe një kërkesë për të dhënë një emër të vërtetë [6]. Nëse ne për kryerjen e një pagese përdorim kartën e debitit sigurinë për kryerjen e veprimit e jep banka dhe nëpërmjet marrjes së konfirmimit nga banka kryhet dhe transkaksioni, ndërsa kur ti përdor monedhën e bitcoin-it asnjë institucion financiar nuk jep dakordësinë për kryerjen e veprimit, si rrjedhojë ti si individ nuk e kupton në mënyrë të mirëfilltë veprimin që kryhet duke qenë se ti thjesht lexon një kod kompjuterik të zakonshëm.

2. Efektet pozitive dhe negative të kriptomonedhave

Revolucioni teknologjik që po përjetojmë vitet e fundit konsiston edhe ndër të tjera pikërisht në zhvillimin e monedhave digjitale. Në ditët e sotme kemi një sërë monedhash digjitale sic janë Bitcoin, Ether, Matik, Dogecoin, janë diku te 8000 lloje kripto nga të cilat jo të gjitha janë me vlerë, Bitcoin është monedha që ka më shumë vlerë, ku vlera e saj ka shkuar edhe 70 mijë dollarë. Po shohim që gjithnjë e më shumë njerëzit po blejnë monedha virtuale ku ndër më me vlerë është pikërisht Bitcoin dhe Ether. Sa më shumë të blejnë njerëzit monedha të tilla aq më shumë ju rritet vlera. Një e veçantë tjetër e kriptomonedhës që ka një rëndësi të madhe në përdorim por edhe

4 The economist. The great chain of being sure about things https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

5 Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives*, 29 (2): 213-38. DOI: 10.1257/jep.29.2.213 https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

6 Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives*, 29 (2): 213-38. DOI: 10.1257/jep.29.2.213 https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

në rritjen e besimit te njerëzit për ta përdorur gjithnjë e më shumë atë është pikërisht fakti që kriptomonedhat nuk mund të shkatërrohen. Çdo server i veçantë kompjuterik që pret një regjistër ose regjistër të kriptomonedhës mund të shkatërrohet, por ekzistenca e monedhës do të vazhdojë të qëndrojë në server të tjerë në të gjithë botën dhe mund të përsëritet shpejt [7].

Një risk me të cilin mund të hasen zotëruesit e monedhave digjitale është transkanksioni i dyfishtë që do të thotë një individ është në gjendje të lëshojë dy transaksione paralele, pra të japi të njëjtën monedhë dy marrësve të ndryshëm [8]. Nëse ti kryen një transaksion të centralizuar dhe online, banka ose sistemi operartiv është në gjendje që të dallojë kur kryhen veprime të dyshimta. Teknologjia blockchain është shumë e sigurt. Mashtruesit nuk mund të kryejnë një krim të tillë sepse nuk mund të ndryshohet as të vërtetojë disa libra në të njëjtën kohë, jo më kot rrjeti blockchain është cilësuar si platforma më e sigurt [9]. Referuar studimit të kryer nga Bentov ekziston mundësia e thyerjes së sigurisë së kriptomonedhave nëse mashtruesit janë në gjendje të kontrollojnë një sasi të madhe të aksioneve në vërtetimin e fuqisë hash të punës[10]. Fuqia hash është fuqia llogaritëse që kontrollon aftësinë ose ndryshe fuqia e nevojshme që kërkohet nga rrjeti i kriptomonedhave që të funksionojnë vazhdimisht. Teorikisht, mashtrimi mund të bëhet në një masë të madhe me kusht që mashtruesit të jenë në gjendje të kontrollojnë në të përqindje të caktuar fuqinë hash[11]. Në rastin e monedhës së bitcoin që të ndodhi një fenomen i tillë duhet që mashtruesi të zotëroje 51% të fuqisë kompjuterike. Algoritmi i përdorur për krijimin e monedhës së bitcoin bën të mundur që përdorimi i saj në transaksione të jetë më i sigurt sesa përdorimi i kartave të kreditit. Mekanizmi i transferimit me kriptomonedha është me autentifikim nga shitësi te blerësi, ky proçes bën të mundur parandalimin për të falsifikuar ndonjë transaksion të ri ose të transanksioneve të rimbursimit. Të dhënat digjitale dhe dokumentet online ruhen në një siguri shumë të lartë

7 https://www.businessinsider.com/positives-and-negatives-of-bitcoin-2016-8

8 F. Tschorsch and B. Scheuerman n, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016, DOI: 10.1109/COMST.2016.2535718;

9 Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. Physica A: Statistical Mechanics and its Applications, 484, 82-90, https:// doi.org/10.1016/j.physa.2017.04.159;

10 Bentov, I., Kumaresan, R. (2014). How to Use Bitcoin to Design Fair Protocols. In: Garay, J.A., Gennaro, R. (eds) Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, vol 8617. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44381-1_24

11 Muhammad Ashraf FAUZI, Norazha PAIMAN, Zarina OTHMAN / Journal of Asian Finance, Economics and Business Vol 7 No 8 (2020) 695–704; doi:10.13106/jafeb.2020.vol7.no8.695;

në databazën e blockchain si për momentin por edhe në të ardhmen.

Kriptomonedhat janë funksionale 24 orë në 7 ditë të javës gjatë gjithë vitit, nga kushdo. Çmimi i të dhënave është në dispozicion në çdo çast ku të gjithë njerëzit në botë nëse duan të tregtojnë diçka e bëjnë pa asnjë kosto për sa kohë që interneti është i aksesueshëm [12]. Aksesimi i lehtë në kriptomonedha ka bërë që besimi te njerëzit të rritet, kjo sjell rritje të vlerave të tyre, të lehtësimit të kryerjes së pagesave të shumta, të zotërimit të parasë virtuale por nga ana tjetër patjetër që krijon skema të ndryshme të veprave penale.

Duhet theksuar se monedhat digjitale përballen edhe me shumë sfida duke u transmetuar edhe te individët të cilët i posedojnë apo që kryejnë veprime me to. Mungesa e legjislacionit dhe krijimi i një organi që kontrollon gjithçka në lidhje me kriptomonedhat bën të mundur krijimin e një sërë aktivitetesh të paligjshme. Mënyra e funksionimit të tyre, anonimati, aksesi nga kushdo krijon një mjedis shumë të përshtatshëm për mashturesit, apo për kryerjen e një sërë veprash penale. Ka vende të cilat e kanë të ndaluar përdorimin e Bitcoin, si psh Kina [13], e cila ka të ndaluar përdorimin e çdo monedhe digjitale të përdorura nga cdo institucion financiar dhe nga cdo lloj biznesi.

Prodhimi i energjisë elektrike nga minimi i kriptomonedhave variojnë nga 10MË, vlerë kjo ekuivalente me një termocentral të vogël, në 3-6 GË, ekuivalente kjo me energjinë e konsumuar nga shtetet e mesme deri në të vogla, siç mund të jenë Bangladeshi dhe Danimarka [14]. Nivelet e larta të prodhimit të energjisë elektrike ndikojnë në mënyrë të drejtpërdrejtë në mjedisin tonë dhe në atë që gjithnjë e më shumë po merr vëmëndje si ngrohja globale. Referuar Berger[15], minierat e kriptomonedhave do të kontribuojnë në emetimin e dioksidit të karbonit dhe do të shkatërronte tokën nëpërmjet ngrohjes globale. Ai sugjeron se duhet të kryhen studime të posaçme për efektet që do të sjellë në plan afatgjatë prodhimi i tyre.

---

12 Pieters, Gina & Vivanco, Sofia, 2017. "**Financial regulations and price inconsistencies across Bitcoin markets**," Information Economics and Policy, Elsevier, vol. 39(C), pages 1-14. DOI: 10.1016/j.infoecopol.2017.02.002

13 Adrian (Wai-Kong) Cheung, Eduardo Roca & Jen-Je Su (2015) Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices, Applied Economics, 47:23, 2348-2358, DOI: 10.1080/00036846.2015.1005827

14 Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability, 28, 1-9; https://doi.org/10.1016/j.cosust.2017.04.011

15 Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can ëe afford integrity by proof-of-ëork? Scenarios inspired by the Bitcoin currency. In: The Economics of Information Security and Privacy (pp. 135-156). Berlin/ Heidelberg, Germany: Springer. https://doi.org/10.1007/978-3-642-39498-0_7

3.Legjislacioni shqiptar për kriptomonedhat

Shqipëria është një nga të paktat vende në Europë e cila ka një ligj i cili rregullon tregun e kriptomonedhave. Ligji nr.66/2020 "Për tregjet financiare të bazuara në teknologjinë e regjistrave të shpërndarë" [16] ka si objekt përcaktimin e rregullave për një biznes ose individ që nga marrja e liçensës deri te dalja në treg si bursë digjitale. Autoriteti i Mbikëqyrjes Financiare dhe AKSHI do të jenë institucionet të cilat do të lëshojnë liçensat për tu bërë pjesë e bursave digjitale. Ligji rregullon proçedurën e aplikimit, të koordinimit midis institucioneve përkatëse, llojeve të liçensave të nevojshme si dhe kriteret që duhet të përmbushen. Ligji është shoqëruar me një rregullore nr.708, datë 24.11.2021[17], ku përcaktohen në mënyrë më të detajuar rregullat që duhet të ndiqen për tu bërë pjesë e tregut të kriptomonedhave. Rregullorja përcakton tre lloj liçensash për bizneset apo për individët, kapitalin minimal që duhet të posedojnë të depozituar në bankë. Theksi vihet edhe në problemin më të madh që ka ky treg, krijimi i skemave për pastrimin e parave. Për këtë arsye parashikohet që çdo titullar liçense të krijojë një sistem të sigurt dhe të mbrojtur nga risqet për të monitoruar transaksionet në përputhje me ligjin për parandalimin e pastrimit të parave dhe financimit të terrorizmit, nëpërmjet hartimit të politikave për parandalimin e pastrimit të parave dhe angazhimit të punonjësve me përvojën e duhur për raportimin e çështjeve që lidhen me parandalimin e pastrimit të parave.

Ekspertët e kriptomonedhave shprehen shumë skeptikë në lidhje me ligjin nr.66/2020 "Për tregjet financiare të bazuara në teknologjinë e regjistrave të shpërndarë" duke u shprehur se ky ligj rregullon pjesën e Exhange-it por jo të prodhimit të kriptovalutave[18]. Krijimi i ligjit ka nxitur më shumë njerëzit që të investojnë në kriptovaluta, vlera e të cilave është shumë lehtë e ndryshueshme duke sjellë një pasiguri të madhe dhe duke i krahasuar ato edhe me skemat piramidale. Kriptovaluta u krijua që të ruajë privatësinë e personit, në momentin që miratojmë ligje dhe vendosim rregulla humb sensi i kësaj paraje digjitale.

16 https://cqbz.gov.al/

17 https://akshi.gov.al/wp-content/uploads/2022/02/vendim-2021-11-24-708.pdf

18 https://euronews.al/kryesore/2022/06/10/eksperti-tregon-disa-nga-skemat-se-si-pastrohen-parate-nepermjet-kriptovalutave/

4. Kriptomonedhat dhe përdorueshmëria e tyre për qëllime kriminale

Sic e shpjeguam në pjesën hyrëse të këtij artikulli, kriptomonedhat po kthehen në mjete shumë të leverdisshme për grupet kriminale për të konsumuar vepra të ndryshme penale. Konkretisht si përdoret bitcoin apo kriptomonedha të tjera për kryerjen e këtyre veprave penale? Një element i rëndësishëm që duhet të theksohet në rastet e kriptomonedhave është fakti se edhe pse janë të enkriptuara përsëri nuk ta ruajnë anonimatin 100% të rasteve.

Pra organet ligjzbatuse i kanë të gjitha mundësitë për të ndjekur dhe ndëshkuar transaksione të dyshimta me kriptomonedha të bëra në hapsirën e internetit. Thënë kjo, në treg qarkullojnë në mënyrë ciklike lloje të ndryshme kriptomonedhash të cilat "premtojnë" fshehtësi dhe anonimat të plotë, ku dhe subjektet me qëllime kriminale kanë gjetur "parajësën e tyre", larg syve vëzhgues të ligjit.

Sipas "Europol" monedha digjitale "Monero" është një nga shumë llojet në qarkullim të monedhave digjitale të cilat ofrojnë anonimat të plotë të transaksioneve midis palëve ashtu edhe fshehtësi të llojit të teknologjisë apo teknikave të përdorura. Monedha të tjera të preferuara nga këto subjekte përshijnë Dash dhe Zcash të cilat njëlloj si Monero premtojnë fshehtësi dhe diskrecion të plotë të përdoruesve të tyre. [19]

Me kalimin e kohës, tregu i kriptomonedhave është diversifikuar mjaftueshëm, megjithatë Bitcoin përsëri mbetet kriptomonedha mbizotëruese në treg, dhe zë rreth 44% të të gjithë tregut. Monedhat e tjera digjitale nuk ja kanë dalë të kenë të njëjtin impakt apo të jenë njëlloj po aq likuide sa Bitcoin, dhe kjo është edhe arsyeja që shpeshherë ndodhin ulje dhe ngritje të konsiderueshme të vlerave të tyre në bursë duke sjellë kësisoj edhe fitime apo humbje kolosale për posueduesit e tyre.

Në ditët e sotme gjithnjë e më shumë kompani po pranojnë të kryejnë transaksione me Bitcoin. Gjigandi i transaksioneve ekonomike në botë "PayPal" në qershor të këtij viti pranoi të fillonte kryerjen e transaksionve me Bitcoins. Tashmë përdoruesit e "PayPal" kanë mundësinë të kryejnë transaksione të ndryshme me Bitcoin nga llogaritë e tyre "PayPal" dhe portofolëve digjital. [20]

19 Europol Spotlight: "Europol tracing the evolution of criminal minds", fq 6-7

20 PayPal Users Can Noë Transfer, Send, and Receive Bitcoin, Ethereum, Bitcoin Cash, and Litecoin https://newsroom.paypal-corp.com/2022-06-07-PayPal-Users-Can-Noë-Transfer-Send-and-Receive-Bitcoin-Ethereum-Bitcoin-Cash-and-Litecoin (aksesuar për herë të fundit

Në seksionet vijuese të punimit do ti referohemi veprave penale konkrete apo ngjarjve kriminale konkrete të cilat janë konsumuar duke patur për bazë kriptomonedhat dhe pasojat që kanë ardhur si rrjedhojë e përdorimit të tyre.

4.1 Përdorimi praktik i kriptomonedhave nga subjektet kriminale

Në pjesën e parë kemi folur lidhur me kriptomonedhat dhe rëndësinë, impaktin dhe përdorueshmërinë e tyrë. Por pyetja më e rëndësishme nga të gjitha është si përdoren kriptomonedhat në botën apo nga subjektet kriminale? Le ti hedhim një sy disa prej veprave penale më të zakonshme të cilat kanë për element përbërës të tyre kriptomonedhat e ndryshme.

4.2 Skemat mashtruese dhe piramidale me kriptomonedha

Në Kodin Penal të Republikës së Shqipërisë në nenin 143/a parashikohet pikërisht skemat mashtruese dhe piramidale. Kuptohet Kodi jonë bën një parashikim të përgjithshëm për skemat mashtruese piramidale pa u futur në detaje lidhur me mjetet sesi mund të realizohet kjo. Për të kuptuar në përgjithësi se cfarë janë skemat mashtruese dhe piramidale është e nevojshme të kuptojmë se si janë të organizuara këto skema dhe sesi konsumohen nga ana objektive.

Skemat piramidale janë modele biznesi, ku një subjekt krijon një shoqëri tregtare dhe bind subjekte të tjera të invesojnë në shoqërinë e tij/saj. Investimi që viktimat bënin në këtë shoqëri ishte një investim i konsiderueshëm, i cili më pas premtohej se do të kthehej në përqindje fitimi të konsiderueshme ndaj investitorëve. Kuptohet se ky investim nuk kthehej kurrë dhe viktimat e mashtrimit pësonin humbje të mëdha financiare. Skemat primadale dhe mashtruese nuk janë shpikje e vonë, ka të dhëna se këto skema kanë ekzistuar që në shekullin e XIX dhe padyshim skema më e famshme është skema Ponzi e krijuar në dhjetor të vitit 1919.[21]

Thënë kjo le ti rikthehemi diskutimit lidhur me kriptomonedhat dhe përdorimin e tyrë në këto lloj skemash mashtruese.

Në 2011 Europol në bashkëpunim me Eurojus, pas një hetimi disa mujor kanë arritur të arrestojnë pjesëtarët e një grupi kriminal i cili merrej me

---

më 10.06.2022)

21 "When did it begin?" Encyclopedia.com https://www.encyclopedia.com/finance/encyclopedias-almanacs-transcripts-and-maps/pyramid-scheme#:~:text=When%20Did%20It%20Begin%3F,Ponzi%20(1882%E2%80%931949). (aksesuar për herë të fundit më 15.06.2022)

investimet me risk të lartë në kriptomonedha online.[22] Grupi kishte krijuar të paktën 4 platforma të tilla online ku, mashtronin viktimat. Ata paraqiteshin si agjent shitjesh ekspert dhe kontaktonin personalisht viktimat me anë të një call centeri që kishin organizuar dhe i tregonin të dhëna të manipuluara ku shfaqeshin fitime të mëdha për investitorët e platfromave të tyre. Viktimave u kërkohej të investonin në kriptomonedha të ndryshme por kryesisht Bitcoin, ku dhe ju premtohej kthim fitimesh te konsiderueshme. Kësisoj u arrit të mashtrohen një numër i konsiderueshëm viktimash, të cilët gjithashtu pësuan humbje që përllogariten me rreth 30 milion euro.[23]

Një tjetër rast i skemave mashtruese dhe piramidale me anë të kriptomonedhave është gjithashtu edhe rasti i skemës Ponzi "Vitae". Ngjashëm me rastin e mësipërm edhe këtu subjektet e kësaj vepre penale, kishin krijuar një platformë online në të cilën arrinin të kontaktonin viktimat për ti bindur të investonin në skemën e tyre. Mendohet se kanë rënë viktimë e këtyre skemave priamidale mashtruese rreth 223 000 individ nga 177 vende të botës.[24]

4.3 Pastrimi i produkteve të veprës penale apo veprimtarisë kriminale me kriptomonedha

Në korrik 2017, në Kaliforni të Shteteve të Bashkuara të Amerikës, u gjend fajtor një shtetas rus për veprat penale të pastrmit të produkteve të veprës penale, krimi kibernetik dhe ransomëare.[25]

Ky subjekt kishte krijuar disa llogari BTC-e të cilat përdoren për këmbimin e kriptomonedhave dhe monedhave të tjera tradicionale. Në momentin e ndodhjes së kësaj ngjarje nuk ka patur një rregullim të saktë lidhur me këto kompani të cilat merren vetëm me procesin e shkëmbimit të monedhave të tjera me bitcoin, ndaj dhe operimi i tyre online nuk ka qenë i lejuar. Megjithatë, subjekti në fjalë nuk kishte vepruar vetëm këtu. Ai

22 "Trading scheme resulted in 30 million losses uncovered" Europol https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-%e2%82%ac30-million-in-losses-uncovered (aksesuar për herë të fundit më 15.06.2022)

23 Po aty

24 Europol helps Belgian and Swiss authorities unravel Vitae Ponzi Scheme https://www.europol.europa.eu/media-press/newsroom/news/europol-helps-belgian-and-sëiss-authorities-unravel-vitae-ponzi-scheme (akesuar për herë të fundit më 15.06.2022)

25 Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged (akesuar per herë të fundit më 15.06.2022

përvec se operonte këto lloj llogarish pa kurrëfarë kontrolli dhe mbikqyrjeje nga autoritetet, arrinte të vidhte identitetet e viktimave online dhe më pas i shantazhonte se do ti bënte publike (ransomëare). Krijonte lehtësisra të konsiderueshme për blerjen apo shitjen e lëndëve narkotike online nëpërmjet Bitcoin dhe gjithashtu mundësonte pastrimin e produkteve të veprës penale nëprmjet transferimeve dhe këmbimeve të cilat bëheshin pa asnjë lloj kontrolli.

Në ditët e sotme shtetet janë përpjekur ti japin një zgjidhje dhe një rregullim më të posacëm këtyre shërbimeve për shkëmbimn e kriptomonedhave. Në Bashkimin Europian janë ligjëruar dhe disiplinohen nga i njëjti kuadër rregullator si bankat.[26]

Raporti i Europol lidhur me pastrimin e parave citon se kriptomonedhat janë kthyer ndër metodat e preferuara për keqbërësit për pastrimin e produkteve të veprës penale. Aktivitet ky i cili arriti një pikë kulmore me pandemin e shkaktuar nga COVID-19. Në dark ëeb bëhet shpesh reklamim i shërbimeve të cilat ofrojnë shkëmbime të kriptomonedhave në monedha të tjera dhe gjithashtu japin informacion sesi mundet që këto subjekte të bëhen posedues të "ligjshëm" të këtyre shumave të parave. Një ndër metodat e më të zakonshme është shkëmbimi i Bitcoins në kupona dhuratash ose kthimin e tyre në karta debiti të parapaguara.[27]

4.4 "Angazhimi" i vrasësve me pagesë në dark ëeb

Duke ju rikthyer edhe një herë çështjes së anonimatit, dhe mundësisë që kritpomonedhat e llojeve të ndryshme të japin për tu fshehur në mënyrë thuajse perfekte online, janë vërtetuar edhe raste kur janë "punësuar" ose "angazhuar" vrasës me pagesë online. Ky është rasti i një shtetasi itialian i cili pagoi 10.000 euro në Bitcoin për të gjetur një vrasës me pagesë, i cili do të vriste ish-partneren e tij.[28] Autoritetet italiane në bashkëpunim me organizata të tjera ligjzbatuese Europiane, bën një analizim kompleks të kriptove me qëllim identifikimin e porositësit të këtij krimi.

26 Europol Spotlight: "Europol tracing the evolution of criminal minds" fq 8

27 Po aty, fq 12

28 "Dark web hitman identified through crypto analysis" https://www.europol.europa.eu/media-press/neësroom/neës/dark-ëeb-hitman-identified-through-crypto-analysis (aksesuar për herë të fundit më 16.06.2022)

Përfundime

Përdorimi i kriptomonedhave patjetër që shënon një arritje të madhe në fushën teknologjike, të ekonomisë, të krijimit të një monedhe virtuale apo edhe të një portofoli virtual. Megjithatë paralelisht mund të themi se kriptomonedhat kanë krijuar edhe një ambjent totalisht të sigurt për favorizimin e kryerjes së veprave penale të ndryshme.

Thirrjet e shumë ekspertëve janë pikërisht ngritja e alarmit për inevstimet në kriptomonedha. Shumë prej tyre i kanë krahasuar me skemat piramidale, dhe mbi të gjitha shumë individë kanë përdorur pikërisht modelet e skemave piramidale për të mashtruar një sërë njerëzish duke i bindur të investojnë në kriptomonedha.

Ekspertët theksojnë gjithashtu se investimi në kriptomonedha ka shërbyer edhe si një mjet efikas pikërisht për pastrimin e produkteve të veprës penale, kjo duke sjellë një siguri te të gjithë personat që kryejnë veprimtari kriminale. Për këto arsye gjithnjë e më shumë nevojitet një studim më i thelluar, më shumë informacion, dhe mbi të gjitha ngritja e mekanizmave të duhur për kontrollimin e veprimtarisë së kriptomonedhave. E nevojshme është edhe harmonizimi i akteve ligjore me ngritjen e institucioneve përkatëse për të parandaluar efektet negative dhe zgjerimin e fushës kriminale që kriptomonedhat po lejojnë të krijohen dhe të ndodhin në të gjithë botën. Do të kish qenë e udhës së përparimi i teknogjisë të shoqërohet edhe me mjetet e duhura për parandalimin e krijimit të skemave të ndryshme kriminale.

Tentativat e vendeve të ndryshme të botës është rregullimi ligjor i posaçëm i monedhave digjitale dhe "tregjet" online ku ato blihen, shiten dhe këmbehen me monedha të tjera më tradicionale. Në Shqipëri ka pasur pak përparim në këtë fushë duke hartuar një ligj specifik vetëm për rregullimin e këtyre veprimtarive. Megjithatë, legjislacioni shqiptar ka nevojë për miratimin e akteve nënligjore shtesë të cilat do të shërbejnë edhe për një rregullim më efikas të prodhimit dhe tregtimit të kriptomonedhave në vendin tonë.

Referenca

Kayal, P., Rohilla, P. Bitcoin in the economics and finance literature: a survey. *SN Bus Econ* **1,** 88 (2021). https://doi.org/10.1007/s43546-021-00090-5, aksesuar për herë të fundit më 13.07.2022

The economist. The great chain of being sure about things https://www.

economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, aksesuar për herë të fundit më 13.07.2022

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives*, 29 (2): 213-38. DOI: 10.1257/jep.29.2.213 https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213 akesuar për herë të fundit më 13.07.2022

F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016, DOI: 10.1109/COMST.2016.2535718; akesuar për herë të fundit më 13.07.2022

- Bariviera, A. F., Basgall, M. J., Hasperué, Ë., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. Physica A: Statistical Mechanics and its Applications, 484, 82-90, https:// doi.org/10.1016/j.physa.2017.04.159; akesuar për herë të fundit më 13.07.2022

Bentov, I., Kumaresan, R. (2014). Hoë to Use Bitcoin to Design Fair Protocols. In: Garay, J.A., Gennaro, R. (eds) Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, vol 8617. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44381-1_24 akesuar për herë të fundit më 13.07.2022

- Muhammad Ashraf FAUZI, Norazha PAIMAN, Zarina OTHMAN / Journal of Asian Finance, Economics and Business Vol 7 No 8 (2020) 695–704; doi:10.13106/jafeb.2020.vol7.no8.695;
- Europol Spotlight: "Europol tracing the evolution of criminal minds", fq 6-7

PayPal Users Can Noë Transfer, Send, and Receive Bitcoin, Ethereum, Bitcoin Cash, and Litecoin https://newsroom.paypal-corp.com/2022-06-07-PayPal-Users-Can-Noë-Transfer-Send-and-Receive-Bitcoin-Ethereum-Bitcoin-Cash-and-Litecoin (aksesuar për herë të fundit më 10.06.2022)

"When did it begin?" Encyclopedia.com https://www.encyclopedia.com/finance/encyclopedias-almanacs-transcripts-and-maps/pyramid-scheme#:~:text=Ëhen%20Did%20It%20Begin%3F,Ponzi%20(1882%E2%80%931949). (aksesuar për herë të fundit më 15.06.2022)

"Trading scheme resulted in 30 million losses uncovered" Europol https://www.europol.europa.eu/media-press/neësroom/news/trading-scheme-resulting-in-%e2%82%ac30-million-in-losses-uncovered (aksesuar për herë

të fundit më 15.06.2022)

Europol helps Belgian and Sëiss authorities unravel Vitae Ponzi Scheme https://www.europol.europa.eu/media-press/neësroom/news/europol-helps-belgian-and-sëiss-authorities-unravel-vitae-ponzi-scheme (akesuar për herë të fundit më 15.06.2022)

Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged (akesuar per herë të fundit më 15.06.2022

- Europol Spotlight: "Europol tracing the evolution of criminal minds" fq 8

"Dark web hitman identified through crypto analysis" https://www.europol.europa.eu/media-press/newsroom/news/dark-ëeb-hitman-identified-through-crypto-analysis (aksesuar për herë të fundit më 16.06.2022)

FACIAL RECOGNITION TECHNOLOGY (FRT): PROS AND CONS OF USAGE IN LAW ENFORCEMENT AGENCIES

LLM. KLEA XHAFERI (ASSISTANT LAWYER)

kxhaferi40@gmail.com

Abstract

Facial Recognition is a technology that uses a method of biometric identification to verify or authenticate a person using a photo or video. Recent advancements in FRT, such as its use in realtime, create new opportunities to leverage the technology for increased public safety. In the digital world that we are living, if FTR is used under specific provisions and control systems, it could help law enforcement agencies deter terrorism, prevent violent crime, identify wanted individuals, find missing persons, and assist in post-event investigations.

Certain countries are using or evaluating the effectiveness of FRT, which has significantly improved in recent years, in part because of the development of high-definition video, advancements in storage capabilities, and the ability to evaluate faces in real time. Some other countries have opposed the idea of FRT usage in law enforcement agencies, due to issues concerning privacy, data security, criminal justice, and human rights.

This paper examines the advantages of this technology if used by the law enforcement agencies in criminal proceedings, as well as possible disadvantages that may affect the outcome of this digital tool. This paper proposes that although privacy considerations or possible deprivation of human rights may exist, the benefits of FTR technology outweigh these concerns. Also, in caseof FRT being used by law enforcement agencies, the above shall be required by governmental bodies to follow certain guidelines,

to prevent such possible risks that may derive from FRT usage.

Key words: Facial Recognition Technology, criminal procedures, privacy, criminal justice,human rights.

1. Introduction

Facial recognitions a few years ago now, may have seemed like a far-off future technology in scient – fiction movies, yet today it is widely used in our daily life. It has now become a useful tool widely used in tech applications to facilitate user`s authentication and recognition, without having to use other types of configurations. Providers like Amazon, Microsoft and IBM have halted both the development and sale of facial recognition technology.

This novel technology constitutes its usage and results in biometric data. Biometric data under European legislation is defined as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data".[1]

Physical characteristics have been one of the oldest and most basic examples of a characteristic that is used for recognition and distinction of humans. Since the beginning of civilization, humans have used faces to identify known and unknown or unfamiliar individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into- once small communities.

The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis.

After industrial revolution, with the rapid growth of cities, there was a formally recognized need to identify people. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of the two approaches was the Bertillon system of measuring various body dimensions, which

1 Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

originated in France[2]. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometries.

The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualized metric- fingerprint patterns and ridges[3]. The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, Bengal, India. [4] and variations on it are still in use for classifying fingerprints.

True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems. The first semi-automatic face recognition system was developed by Woodrow W. Bledsoe under contract to the US Government[5]. This system required the administrator to locate features such as eyes, ears, nose, and mouth on the photographs. This system relied solely on the ability to extract useable feature points. Due to the technological developments, this method has now advanced in fully automated processes that allow identification of a human`s face.

Nowadays the subject of facial recognition is very debatable amongst international institutions and even countries themselves. FRT has integrated into our everyday lives, creating new social benefits around the world. With recent advancements in FRT, law enforcement, governments, and the private sector all look to leverage the technology to make their operations more secure, more efficient and in some cases more profitable for the society.

Still, there is no unified position on a regional level. There are those who have adopted this technology in their public policies, especially in law enforcement technologies; there are also countries such as United Kingdom, which for example by the Court of Appeal has deemed this technology as unlawful, stating that is violates human rights, data protection laws and equality law.[6]

2 Alphonse Bertillion (archive.org) accessed on 30 of June 2022, 11:44 A.M.

3 History of Biometrics | Biometric Update accessed on 30 of June 2022 1:00 P.M.

4 Wayback Machine (archive.org) accessed on 30 of June 2022, 1:15 P.M.

5 History of Biometrics | Biometric Update accessed on 30 of June 2022, 1:35 P.M.

6 See: Case No: C1/2019/2670, Decision of Royal Courts of Justice, date 11.08.2020.

2. What is Facial Recognition Technology (FRT)?

Facial recognition technologies are biometric systems that allow the automatic identification and matching of a person's face. The technology extracts and further processes biometric data by creating a 'biometric template'.[7] For facial images, a biometric template[8] detects and measures various facial features.

Facial recognition is the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorization of those individuals".[9]

Facial recognition refers to a multitude of technologies that can perform different tasks for different purposes. In this regard, a key distinction is whether facial recognition is used for verification, identification, or categorization. Verification and identification deal with matching unique characteristics of individuals to determine their individual identity. Categorization deals with deducing whether an individual belongs to a specific group based on his or her biometric characteristics – for example, sex, age, or race.

In the past few years, facial recognition technologies have strongly benefitted from increased data availability, computing power and the development of sophisticated machine learning algorithms. There exists three types of FRT based on what they deliver as a result of their usage:

2.1 Verification (one to one comparison):

Verification or authentication is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual.[10] Two biometric templates are compared to determine if the person shown on the two images is the same person. Such a procedure is, for example, used at Automated Border Control (ABC) gates

7 Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/ EN, WP193, Brussels, 27 April 2012.

8 'Biometric template' means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications (see Art. 4 (12) of Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, pp. 85-135).

9 Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/ EN, WP193, Brussels, 27 April 2012.

10 Iglezakis, I. (2013)EU Data Protection Legislation and Case-Law with Regard to Biometric Applications by Ioannis Iglezakis :: SSRN, Aristotle University of Thessaloniki, 18 June 2013.

used for border checks at airports. A person scans his or her passport image and a live image is taken on the spot. The facial recognition technology compares the two facial images and if the likelihood that the two images show the same person is above a certain threshold, the identity is verified. Verification does not demand that the biometric features be deposited in a central database. They may be stored, for example, on a card or in an identity/travel document of an individual.

2.2 Identification (one to many comparison):

Identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there. The facial recognition technology returns a score for each comparison indicating the likelihood that two images refer to the same person. Sometimes images are checked against databases, where it is known that the reference person is in the database (closed-set identification), and sometimes, where this is not known (open-set identification). The latter operation would be applied when persons are checked against watchlists. Using facial recognition technology for identification is sometimes referred to as Automated Facial Recognition (AFR)[11]. Identification can be used based on facial images obtained from video cameras. For this purpose, the system first needs to detect if there is a face on the video footage.

Smart phone users might know when taking pictures that sometimes the camera automatically draws rectangles over faces. Faces on video footage are extracted and then compared against the facial images in the reference database to identify whether the person on the video footage is in the database of images (e.g. on the watchlist). Such systems are referred to as Live Facial Recognition Technology (LFRT).[12] The quality of the facial images extracted from video cameras cannot be controlled: light, distance and position of the person captured on the video footage limit the facial features. Therefore, live facial recognition technologies are more likely to result in false matches as compared to facial images taken in a controlled environment, such as a border crossing point or a police station.

---

11 Davies, B., Innes, M., and Dawson, A. (2018), An Evaluation of South Wales Police's use of Automated Facial Recognition, Cardiff University, September 2018, accessed on 1 July 2022, 1:00 P.M. AFR+Report+[Digital].pdf (squarespace.com)

12 Fussey, P. and Murray, D. (2019), Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, July 2019: 56524_A4 Booklet HRBDT report_V3_web.pdf (netdna-ssl.com); accessed on 1 July 2022 1:15 P.M.

2.3 Categorization (matching general characteristics):

Apart from verification and identification, facial recognition technology is also used to extract information about an individual's characteristics. This is sometimes referred to as "face analyses". It can, therefore, also be used for profiling individuals, which involves categorizing individuals based on their personal characteristics. Characteristics commonly predicted from facial images are sex, age and ethnic origin. Categorization means that the technology is not used to identify or match individuals, but only characteristics of individuals, which do not necessarily allow for identification. However, if several characteristics are inferred from a face, and potentially linked to other data (e.g., location data), it could *de facto* enable the identification of an individual.

3. Use of FRT by public authorities in the European countries

Fundamental Rights Agency (FRA) has conducted deep research in public authorities in European countries about their possible use and plans of using live facial recognition technologies for law enforcement purposes.

On their conclusions on the report[13], German and French authorities have tested live facial recognition technologies only on volunteers, without clearly indicating who would be included on watchlists if the technology were to be used for real deployments. Due to the absence of a legal basis for their deployment, live facial recognition technologies could currently not be used legally in these two countries.

So far, the police in the United Kingdom has been most active in experimenting with live facial recognition technologies. The London Metropolitan Police conducted ten live facial recognition technologies test deployments between 2016 and 2019 in order to test how effectively facial recognition technologies can identify individuals on watchlists.[14] They raised concerns with respect to the integrity of the databases from which images were taken for the watchlists, and the fact that images were drawn from other sources as well[15].Civil society criticized the lack of information on

13 Facial recognition technology: fundamental rights considerations in the context of law enforcement (ISBN 978-92-9474-838-6, doi:10.2811/524628) Facial recognition technology: fundamental rights considerations n the context of law enforcement (europa.eu) accessed on 1 July 2022 1:45 P.M.

14 Ibid.

15 London Policing Ethics Panel (2018), Interim Report on Live Facial Recognition: lpep_report__

who is on the watchlists due to the absence of legislation or guidance. Later on August 11, 2020, the Court of Appeal of England and Wales overturned the High Court's dismissal of a challenge to South Wales Police's use of Automated Facial Recognition technology ("AFR"), finding that its use was unlawful and violated human rights.

The police in Nice (France) conducted a trial of live facial recognition technologies at the carnival in 2018.[16] The purpose of the test was to assess the technology's efficiency. The 'watchlist' of the trial consisted of images of volunteers. People at the carnival could choose whether to enter the area where live facial recognition technologies was being deployed. The Gendarmerie in France has been using facial recognition technologies for criminal investigations but does not use live facial recognition technologies due to the absence of a legal basis to do so.

These tests show that a number of Member States are interested in the potential use of facial recognition technologies, whether live or not. In some cases, the testing is evaluated either by independent entities contracted by the police, or by the police themselves. Experts interviewed by FRA has mentioned that potential future use of facial recognition technologies for the police could target only large events and gatherings as well as everyday security at public places.

Still, civil society, data protection authorities and academics have raised several fundamental rights concerns with respect to the use of facial recognition technologies. Fundamental rights concerns in relation to the potential use of facial recognition technologies, with a focus on live facial recognition technologies will be discussed below.

4. Benefits of law enforcement agencies derived from use of FRT

The most important benefits derived from the use of FRT all involve preventing and reducing crime: prevention of crimes, investigative assistance, potentially terrorism prevention and rapid wanted person identifications.

---

live_facial_recognition.pdf (policingethicspanel.london) accessed on 1 July 2022 1:55 P.M.

16 Facial recognition technology: fundamental rights considerations in the context of law enforcement (ISBN 978-92-9474-838-6, doi:10.2811/524628) Facial recognition technology: fundamental rights considerations n the context of law enforcement (europa.eu) accessed on 1 July 2022 1:45 P.M.

4.1. Preventing violent crime

Like fingerprints and DNA, FRT technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances.

If using FRT in law enforcement agencies, a database would have to be created populated by individuals with criminal records or known for exhibiting compulsive behavior toward public figures. This can prove as a proactive approach to mitigating potential safety concerns at large- scale, high-profile events.

4.2. Investigating and preventing acts of terrorism

FRT can also identify and alert police officer to the presence of a known terrorist entering or exiting a specific location. Furthermore, using live FRT in subway or transport systems, would enable law enforcement agencies to screen millions of people each day and potentially identify individuals on terror watch lists.

Countries like Germany, are testing real- time FRT in the Berlin stations, contending that the technology can alert police of known terrorism suspects.[17] Although no acts of terrorism have been successfully prevented using FRT, law enforcement professional are of the opinion that because of recent technological advancements, using FRT in real-time may prevent an act of terrorism.

4.3. Real- time identifications of wanted persons and known suspects

FRT can be widely used to identify wanted persons and known aspects. Instant identifications of individuals have the potential benefits of making the airline industry safer, locating missing children and adults, and helping instantly to apprehend individuals wanted for serious crimes.

Several companies contend that using FRT in real-time can have the advantage of using it in a variety of platforms, such as the military, law enforcement and the private sector. Technologies such as NEC (NeoFace watch) contend that their facial recognition software is accurate with real-

17 Justin Huggler, "Facial Recognition Software to Catch Terrorists Being Tested at Berlin Station," Telegraph, August 2, 2017, Facial recognition software to catch terrorists being tested at Berlin station (telegraph.co.uk) accessed on 2 July 2022, 10:00 A.M.

time functionality, regardless of various angles and lighting.[18]

4.4. Investigative assistance

Law enforcement agencies with FRT would have the capability to leverage this kind of technology as a post-investigative tool. The resources of FRT databases would be a great aid in criminal investigations to identify perpetrators involved in crimes and to identify deceased and unidentified persons.

4.5. Other law enforcement and public benefits

In addition to crime-prevention benefits, using FRT may increase officer safety, assist officers in the field when interacting with individuals who cannot care for themselves, and help locate missing persons.

If FRT is to be used by law enforcement agencies, the information provided to the police officers can be integrated with other technologies such as License Plate Reader. Therefore, the officers will have more information when interacting with individuals, such as persons wanted for murder or who have prior arrests for assaulting police officers. In addition, officer stops can be expedited if citizen identification are validated in the field.

In addition to that, this technology can assist officers in helping individuals who might be unable to care for themselves, or even find missing persons included in their databases.

5. Potential challenges in using FRT by law enforcement agencies

The use of facial recognition technology entails both risks and opportunities for fundamental rights. It entails many fundamental rights challenges that result from the weak position of the individuals whose facial images are captured and then checked against a 'watchlist'. This section will be focused on the risks that this technology entails and what possible fundamental rights can be implicated by them.

18 NEC Global Face Recognition Centre of Excellence, NeoFace Watch, High Performance Face Recognition (NEC Global Face Recognition Centre of Excellence, 2016), NEC Global accessed on 4 July 2022, 11:25 A.M.

5.1. The risk of wrong identification

Determining the necessary level of accuracy of facial recognition software is challenging: there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01 %) still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others. There are different ways to calculate and interpret error rates, so caution is required. In addition, when it comes to accuracy and errors, questions in relation to how easily a system can be tricked by, for example, fake face images (called 'spoofing'[19]) are important particularly for law enforcement purposes.

Facial recognition technologies, like other machine-learning algorithms, have binary outcomes, meaning that there are two possible outcomes. It is therefore useful to distinguish between false positives and false negatives:

- A 'false positive' refers to the situation where an image is falsely matched to another image on the watchlist. In the law enforcement context, this would mean that a person is wrongly identified as being on the watchlist by the system, posing real threat to the system of criminal justice.
- False negatives are those who are deemed not to be matches (i.e. not on the watchlist), but in fact are matches. The corresponding "false negative identification rate", or "miss rate", indicates the proportion of those erroneously not identified among those who should be identified.

The issue of false positives and false negatives is also connected to data quality and to the accuracy of data processing. Addressing this requires a regular correction and updating of the facial images stored in a watchlist in order to ensure accurate processing.

5.2. Privacy and protection of personal data

The rights to respect for private life and data protection are central to the deployment of facial recognition technology in public places. It is generally agreed that FRT-derived biometric data is information of an intrinsically

19 See for example: Parkin, A. and Grinchuk O. (2019), Recognizing Multi-Modal Face Spoofing With Face Recognition Networks (thecvf.com) accessed on 10 July 9:00 P.M.

private character. And the fact that this biometric data is derived from a person`s facial features that are manifested in public, does not detract from that.

Using live facial recognition technologies implies collecting, comparing and/or storing facial images in an IT system for identification purposes. It, therefore, constitutes an interference with the right to protection of personal data set out in Article 8 of the Charter of the Fundamental Rights of the European Union and the right to private life under Article 7 of the Charter and Article 8 of the European Convention on Human Rights. Facial images constitute personal data, as also confirmed by the CJEU[20] and the ECtHR.[21] The ECtHR has also stated that: "*A person's facial image constitutes one of the key attributes of his/her personality, as it reveals the person's unique characteristics and distinguishes the person from his/her peers. The right to the protection of one's facial image is thus one of the essential components of personal development*."[22]

Nevertheless, jurisprudence has always found a point in the middle of public security and the right of privacy. Usage of FRT can be argued that if used in accordance with the law can become "reasonable expectation of privacy". The processing of facial images in large-scale databases may, as facial recognition technology develops, raise unchartered issues about the rights to protection of private life as well as of personal data. Given that these two rights are not absolute rights, they can be subject to limitations, but any interference needs to be adequately justified[23] and cannot compromise at any event the essential core of that right.

5.3. Misuse

Critics express significant concerns that law enforcement officers may intentionally misuse FRT for personal gain and inappropriately share confidential information. Real-time identification of strangers, including victims of stalking or domestic violence, if used for not legitimate purposes, can pose a lot of risks to the right of privacy and personal data. Like License Plate Reader technology scans when officers use state databases to conduct

20 CJEU, C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013, paras. 22, 48-49.

21 ECtHR, Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 56.

22 ECtHR, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, Strasbourg, Council of Europe, 31 August 2019, para. 138.

23 *Ibid*.

name checks, officers using FRT would be able to obtain personal data that if misused, may incur departmental and criminal sanctions. In addition, critics raise concerns that law enforcement's use of FRT may cause racial bias toward minorities.

5.4. Data storage, data sharing and hacking

With the evolution of cloud technology and the ability to store large amounts of data, law enforcement organizations are challenged with risks to stored information that may be compromised. Each piece of collected information, if compromised, may be used improperly. Government databases are often the biggest target for hackers, facing daily cyber threats that are unique because of potential harm that stolen information inflicts on citizens, such as Albania has recently been affected by data leakage of personal data of Albanian citizens.

6. Requirement that FRT should comply with to justify interference with fundamental rights

Full compliance with fundamental rights is a prerequisite for any law enforcement activities, irrespective of the technologies used. EU and international human rights law provide a normative framework for the design, development, and deployment of facial recognition technologies. They help determine whether a specific use of facial recognition technology is human rights compliant.

An important way to promote compliance with fundamental rights is oversight by independent bodies. Independent supervision is also an essential component of European data protection law,[24]with Article 8 (3) of the Charter of the EU making express reference to it.

Turning to fundamental rights that may be subject to restriction, Article 52 (1) of the Charter sets the framework. Interferences with fundamental rights can only be justified if they respect the requirements of the Charter and of the ECHR, in case of Charter rights corresponding to rights guaranteed in the ECHR (Article 52 (3) of the Charter).

Pursuant to Article 52 (1) of the Charter, any limitation on fundamental rights must:

24 Law Enforcement Directive, Chapter VI; GDPR, Chapter VI.

- be provided for by law,
- genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others,
- respect the essence of the right,
- and be proportionate.

The CJEU has underlined that all of these requirements must be complied with. The court has also emphasized that any limitation on the exercise of the rights and freedoms recognized by in the Charter must respect "the essence" of those rights and freedoms.[25] This means that fundamental rights can be limited to a certain extent, but not completely disregarded. Once it has been established that the inalienable, essential core of a right is not violated by a measure, the necessity and proportionality test as outlined in the Charter is to be conducted as a next step in respect of non-core aspects of that right.

Next to the fundamental rights safeguards and key data protection principles flowing from Article 8 of Charter as interpreted by the CJEU, specific guarantees under the EU data protection acquis further corroborate the necessity and proportionality test. Pursuant to Article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Article 10 of the Law Enforcement Directive lays down similar, albeit a bit more permissive conditions.

Collecting and processing facial images for the purpose of FRT needs to be strictly in line with European data protection law. Following the main legal principles of data protection, processing facial images must be:

- lawful, fair and transparent;
- follow a specific, explicit, and legitimate purpose (clearly defined in Member State or Union law); and
- comply with the requirements of data minimization, data accuracy, storage limitation, data security and accountability.[26]

25 See CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015, paras. 94-95, which refer to Article 52 (3) of the Charter.

26 Law Enforcement Directive, Art. 4; GDPR, Art. 5.

7. Conclusions

This paper tried to give a comprehensive view under the European legal framework of benefits and possible threats of use of Facial Recognition Technology in law enforcement agencies. Finally, it is concluded by the author that although privacy considerations or possible deprivation ofhuman rights may exist, the benefits of FTR technology outweigh these concerns. Also, in case of FRT being used by law enforcement agencies, the above requirement should be taken into consideration to help governmental bodies obey to international law obligations, respect human rights, while also providing a high standard of public security.

Bibliography:

- European Convention on Human Rights.
- Charter of Fundamental Rights of the EU.
- Law Enforcement Directive.
- Regulation (EU) 2018/1725.
- Case No: C1/2019/2670, Decision of Royal Courts of Justice, date 11.08.2020.
- Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/ EN, WP193, Brussels, 27 April 2012.

Davies, B., Innes, M., and Dawson, A. (2018), An Evaluation of South Wales Police's use of Automated Facial Recognition, Cardiff University, September 2018, accessed on 1 July 2022, 1:00 P.M. AFR+Report+[Digital].pdf (squarespace.com).

Fussey, P. and Murray, D. (2019), Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, July 2019: 56524_A4 Booklet HRBDT report_V3_web.pdf (netdna-ssl.com); accessed on 1 July 2022 1:15 P.M.

Iglezakis, I. (2013)EU Data Protection Legislation and Case-Law with Regard to Biometric Applications by Ioannis Iglezakis :: SSRN, Aristotle University of Thessaloniki, 18 June 2013.

London Policing Ethics Panel (2018), Interim Report on Live Facial Recognition: lpep_report__live_facial_recognition.pdf (policingethicspanel.

london) accessed on 1 July 2022 1:55 P.M.

Facial recognition technology: fundamental rights considerations in the context of law enforcement (ISBN 978-92-9474-838-6, doi:10.2811/524628) Facial recognition technology: fundamental rights considerations n the context of law enforcement (europa.eu) accessed on 1 July 2022 1:45 P.M.

Justin Huggler, "Facial Recognition Software to Catch Terrorists Being Tested at Berlin Station," Telegraph, August 2, 2017, Facial recognition software to catch terrorists being tested at Berlin station (telegraph.co.uk) accessed on 2 July 2022, 10:00 A.M.

CJEU, C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013.

CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015.

ECtHR, Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016.

ECtHR, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, Strasbourg, Council of Europe, 31 August 2019.

Alphonse Bertillion (archive.org) accessed on 30 of June 2022, 11:44 A.M.

History of Biometrics | Biometric Update accessed on 30 of June 2022 1:00 P.M

Wayback Machine (archive.org) accessed on 30 of June 2022, 1:15 P.M.

INTELLECTUAL PROPERTY RIGHT AND INTERNET. PROTECTION BY CRIMINAL LEGISLATION IN ALBANIA.

E DREJTA E PRONËSISË INTELEKTUALE DHE INTERNETI. MBROJTJA NGA LEGJISLACIONI PENALE NË SHQIPËRI.

DR. IDLIR DUHANXHI[1]

MSC. MARIGLEN TANUSHI[2]

Abstract!

Intellectual creativity is a very important aspect that has found room in early treatment and protection of the legislation in different countries. Albania, after the '90s, has also become part of the group of these countries that aimed at protecting intellectual property rights. This is an aspect of protecting the interests and rights of the authors of this work and as a very important element of socio-economic development within the country, without leaving out the attention at the international level.

Despite the difficulties encountered in the application of legislation on the protection of intellectual property in Albania, it must be taken into consideration that a good job has been done in terms of consolidating legislation and institutions that focus on this area. The legislatior, through the adoption of intellectual property legislation, has aimed to create a number of protection, both civil and criminal. The period we are going through is accompanied by a "boom" in technology development, especially

in Internet communication, "facilitating" the possibility of distribution and multiplication of materials that are the product of someone else's work and intellectual investment, which should be accompanied by a contemporary improvement of criminal legislation in full coherence with developments.

Exactly the difficulties encountered in the practical application of the legislation in general and the criminal legislation in particular in Albania, by professionals in the field (judges, prosecutors, lawyers), in terms of criminal responsibility by entities that perform actions of this category, will be part of the treatment in this paper.

***Keywords**: Intellectual creativity, copyright, criminal legislation, internet, technological development.*

Abstrakt!

Krijimtaria intelektuale është një aspekt shumë i rëndësishëm që ka gjetur vend herët në trajtimin dhe mbrojtjen e legjislacionit të vendeve të ndryshme. Në grupin e këtyre vendeve që synonin mbrojtjen e të drejtave të pronësisë intelektuale bën pjesë edhe Shqipëria me një zgjerim të kësaj hapësire sidomos pas viteve '90. Ky është një aspekt i mbrojtjes së interesave dhe të drejtave të autorëve të kësaj vepre dhe si një element shumë i rëndësishëm i zhvillimit social-ekonomik brenda vendit, "pa lënë jashtë vëmendjes në nivel ndërkombëtar.

Pavarësisht vështirësive të hasura në zbatimin e legjislacionit për mbrojtjen e pronësisë intelektuale në Shqipëri, duhet pasur parasysh se është bërë një punë e mirë në drejtim të konsolidimit të legjislacionit dhe institucioneve që fokusohen në këtë fushë. Ligjvënësi, nëpërmjet miratimit të legjislacionit për pronësinë intelektuale, ka synuar të krijojë një sërë mbrojtjesh tw natyrës civile dhe penale. Periudha që po kalojmë shoqërohet me një "bum" në zhvillimin e teknologjisë, veçanërisht në komunikimin në internet, duke "lehtësuar" mundësinë e shpërndarjes dhe shumëfishimit të materialeve që janë produkt i punës dhe investimit intelektual të dikujt tjetër, që duhet të shoqërohet me një përmirësim bashkëkohor të legjislacionit penal në koherencë të plotë me zhvillimet.

Pikërisht vështirësitë e hasura në zbatimin praktik të legjislacionit në përgjithësi dhe atij penal në veçanti në Shqipëri, nga profesionistët e fushës (gjyqtarë, prokurorë, avokatë), përsa i përket përgjegjësisë penale nga

subjektet që kryejnë veprime të kësaj kategorie, të jetë pjesë e trajtimit në këtë punim.

Fjalët kyçe: Krijimtaria intelektuale, e drejta e autorit, legjislacioni penal, interneti, zhvillimi teknologjik.

1. MBI LIDHJEN E PRONËSISË INTELEKTUALE ME ZHVILLIMIN E TEKNOLOGJISË.

Zhvillimi i njerëzimit është shoqëruar gjithmonë nga zhvillimi i teknologjisë, që vinte si rezultat i aftësive intelektuale njerëzore *(inteligjencës njerëzore)* për qëllime apo arsye nga më të ndryshme për qëllime civile, por pa përjashtuar dhe luftrat. Shpikjet apo përmirësimet në fushën e teknologjisë, me kalimin e shekujve të cilat sollën një zhvillim të qenësishëm të shoqërisë mbarë botërore në shumë fusha, u panë si një mundësi e madhe, kryesisht të interesave ekonomike të subjekteve që fokusoheshin dhe investonin në fushën e zhvillimit teknologjik. Të shumtë janë shembujt që vinin një theks të rëndësishëm në interesin ekonomik, që solli dhe beteja të shumta mes tyre për të drejtat e shpikjes me rezultat final përveç evoluimit teknologjik edhe interesin ekonomik. Shpikjet dhe risit kanë shoqëruar njerëzimin prej mijëra vitesh, por disa nga shpikjet sollën revolucione të vërteta. Kështu, me shpikjen e shtypëshkronjës nga Guttenberg, u pa një mundësi e shumëfishimit dhe shpërndarjes së informacionit, dijeve që në vetvete u shoqërua me zhvillime dhe shpikje të reja. Për të ardhur tek shpikjet e Nikola Tesla dhe Tomas Edison në fushën e energjisë dhe jo vetëm *(që u shoqërua dhe me përlasje të vazhdueshme mes këtyre të fundit)*. Apo procesi gjyqësor që zgjati mbi një dekate, mes Roberts Kearns që shpiku fshirëset "pulsuese" të xhamave dhe Kompanisë Ford (Chrysler Corporation). që përfundoi me një dëmshpërblim disa miliona dollarësh në favor të Kearns. Rastet e shpikjeve por dhe të cënimit të të drejtave të shpikësve, që në vetvete sillte hezitime apo procedura gjyqësore që nuk mbaronin kurrë, janë të shumta. Pikërisht, duke u evidentuar me rëndësi dhe impakti ekonomik në shoqëri, kjo "simbiozë" është shoqëruar me kërkesën e vazhdueshme të domosdoshmërisë së mbrojtjes të të drejtave dhe të interesave ekonomike të subjekteve zhvillues të kësaj krijimtarie. Kjo me qëllim, që këta të fundit, të jenë më të stimuluar dhe më të garantuar se puna e tyre intelektuale, në risitë që sjellin në teknologjinë dhe shoqërinë njerëzore, nuk do cënohet nga askush dhe kushdo që e qën do "ndëshkohet" për këtë veprim. Në këtë kuadër rrugëtimi, për mënyrën e njohjes dhe të mbrojtjes të të drejtave të pronësisë intelektuale *(në shumë legjislacione të identifikuara si të drejtat e*

autorit dhe të drejtat e lidhur me të dhe ato të pronësisë industriale), erdhi pikërisht si një domosdoshmëri e nevojës për stimulimin e krijimtarisë, kjo me qëllimin e krijimit të këtij ambienti krijimtarie sa më të sigurtë të mundshëm.[1]

Zhvillimi i teknologjisë dhe instrumenteve të shpërndarjes të kësaj krijimtarie të inteligjencës njerëzore, ka qenë i përshkallëzuar në mënyrë progresive. Kështu, shpikje si radio dhe televizori, sollën mundësi të reja, si instrumente të shpërndarjes së informacionit në mënyrë shumë të shpejtë, u shoqërua me domosdoshmërinë e nxjerrjes të një kuadri rregullator në mbrojtje të të drejtave të autorëve për veprat dhe produktet që transmetoheshin nëpërmjet tyre, të cilat përfshinin dhe të drejtat ekonomike. Ky zhvillim solli mundësi dhe këndvështrime të reja në lidhje me të drejtën e pronësisë intelektuale e përfaqësuar nga dy kategori tashmë të pranuara gjerësisht: *1) Të drejtat e autorit dhe të drejtat e lidhura me të; 2) Të drejtat e pronësisë industrial.*

Zhvillimet e dekadave të fundit janë shoqëruar me hapa gjigantë progresiv, pasi zhvillimet e teknologjisë kompjuterike, qw pasuan vitet ’80-’90 dhe në vazhdim, hapi një kapitull të ri, jo vetëm të mënyrës së shpejtë të komunikimit por dhe të një niveli krejt të ndryshëm të të bërit biznes. Kjo e shoqëruar me kërkesën e përmirësimit të kuadrit rregullator (legjislacionit) në përshtatje dhe harmoni me këtë zhvillim, me synimin e mbrojtjes të të drejtave të pronësisë intelektuale. Kjo, për vetë faktin se zhvillimi i teknologjisë kompjuterike (shpikjet si paisjet kompjuterike dhe më pas shpikja e internetit[2]), u shoqërua apo më mirë këto shpikje dhe risi u bën shkak në mundësimin e cënimit më lehtësisht të këtyre të drejtave. Shpërndarja e materiale të fushës letrare dhe industrial, më lehtësisht nga një cep i botës tek tjetri, vuri në pikëpytje faktin se: *Si mundet që të drejtat e*

1 Fillesat e njohjes dhe mbrojtjes së pronësisë intelektuale gjenden në Konventën e Parisit “Për mbrojtjen e Pronësisë Industriale” të vitit 1883 dhe Konventën e Bernës “Për Mbrojtjen e Punëve letrare e artistike” të vitit 1886.

2 Rrjeti apo internet përfaqëson asgjë më shumë se një sërë kompjuterësh të lidhur me njëri tjetrin me kabëll apo ëirles, nëpërmjet një sërë sistemesh softuerësh ose protokollesh dhe adresash të protokollit të internetit apo IP (internet protokoll). Mundësia për të publikuar në formë digjitale e veprave të ndryshme jo vetëm lehtëson por ofron një qasje të shpejtë të publikut të interesuar në internet, në materiale të ndryshme të publikuara nga autorë të ndryshëm. Prandaj, siç përmendëm më sipër, mundësi të tilla të shpëndarjes së këtij informacioni shoqërohet me vështirësi në mbledhjen dhe administrimit të provave,në rastin kur ndodhemi në shkelje të të drejtave të mbrojtura, për të evidentuar dhe provuar ekzistencën e veprimeve penalisht të dënueshme, që do jenë edhe fokusi i këtij punimi. Kjo merr një rëndësi të madhe, duke vështirësuar edhe punën e organeve ligjzbatuese, në rastet kur kemi të bëjmë me subjekte të cilët ndodhen në vende të tjera. Kjo ka rritur kërkesën për bashkëpunim ndërmjet autoriteteve ligjzbatuese të vendeve të ndryshme e shoqëruar dhe me krijimin e organizmave të përbashkët ndërshtetërore.

pronësisë intelektuale të mos cënohen nga zhvillimi i teknologjisë me rëndësi shumë të madhe për njerëzimin siç është interneti apo sëfundmi inteligjenca artificiale?[3] Kjo, është një situatë delikate dhe që kërkon kujdes, njëkohësisht përmirësim të kuadrit rregullator, që bën identifikimin dhe mënyrën se si duhet të veprohet në raste të tilla. Interneti, solli mundësi të shumëfishta për përdoruesit e tij, mundësi të cilat përfaqësoheshin potencialisht nga interesa të mëdha ekonomike, që burimin e kanë pikërisht në shfrytëzimin e këtyre të drejtave të pronësisë intelektuale, në kuadër të marrëdhënieve të ndryshme dhe të shumëfishta ndërmjet përdoruesve të tij. SHBA-të kanë pasur në mënyrë të vijueshme në fokus ruajtjen dhe definimin e saktë të asaj që përbën ose jo cënim të të drejtave të pronësisë intelektuale. Po kështu edhe BE-ja me qasjet që pati, në raport me zhvillimin e komunikimit elektronik, nëpërmjet internetit, u përpoq të riparojë disa pasoja nga kjo teknologji, kjo jo vetëm në këtë sektor por edhe në sektorin e konkurrencës nëpërmjet internetit[4]etj. Në këtë kuadër, u arrit miratimi i Direktivës 2019/790 *(mbi të drejtat e autorit dhe të drejtat e ndërlidhura në Tregun e Vetëm Digjital dhe duke ndryshuar Direktivat 96/9/EC dhe 2001/29/EC, më poshtë Direktiva DSM)*, referuar një procesi miratimi shumë të debatuar dhe me një rezultat që ka sjellë një situatë perceptimi jo të qartë mbi efektet e tij. Pikërisht, duket

3 Duke referuar përdorimin e internetit dhe legjislacionit të miratuar për rregullimin e sektorit të të drejtave të autorit në internet, në horizont sfida tjetër duket se do jetë inteligjenca artificiale (Artificial Intelligence), e cila në vetvete paraqet mundësi cënimi apo deforimimi të parimeve bazë të pronësisë inetelektuale. Nëpërmjet inteligjencës artificiale po krijohen vepra nga më të ndryshmet që në thelb edhe nëse referojnë në një vepër të më parshme, po sjellin risi të cilat e transformojnë një vepër të tillë, duke bërë të pamundur evidentimin nëse jemi para një vepre origjinale apo jo dhe nëse janë cënuar apo jo të drejtat e pronësisë intelektuale. Pikërisht përdorimi i paisjeve të gjenerojnë mundësi të tilla, po tejkalon parashikimet apo kuadrin rregullator aktual, pasi jemi para faktit se këto paisje janë future kaq thellë në jetën tonë sa mundësia për të jetuar pa to është bërë e pamendueshme. Zhvillimi i inteligjencës artificiale po ecën me ritme të jashtëzakonshme, atë e gjejmë kudo në aktivitetin tonë të përditshëm. Mjafton të shohim industrinë e automobilëve që ka njohur një zhvillim të pa parë të kësaj teknologjie, me zëvëndësimin në shumë zinxhirë të prodhimit të punës së njeriut nga makineritë. Vetëm disa dekada më parë nuk mund të imagjinonim drejtimin e autormjetit pa shofer, ndërsa sot ky është një realitet, janë pikërisht kompjuterat që po "mendojnë" apo kujdesen për ne, duke gjeneruar funksione apo arsyetime që deri tani i kemi menduar si veçori vetëm e mendjes njerëzore.

4 Pa u ndalur në këtë trajtim për konkurrencën, duam të evidentojmë se ka një sërë direktivash të BE-së që janë miratuar me fokus rregullimin e tregut në respektim të parimeve të konkurrencës, ku në fokus të tyre ka qenë edhe konkurrenca në treg nëpërmjet shitjeve në internet. Këtu mund të përmendim Direktivën (EU) No. 330/2010. Pikërisht, rastet praktike kanë qenë të shumta në lidhje me mënyrën e trajtimit të tregtimit të produkteve nërpërmjet internertit. Këtu mund të përmendim çështjen C-439/09 Pierre Fabre Dermo Cosmetique (13 October 2011) apo çështjen C-59/08 Copad SA v Christian Dior SA [2009] ECR I-3421 që në fokus kanë pikërisht qasjet dhe aspektin ligjor të respektimit të kushteve dhe rregullave të konkurrencës në treg. – Për më tepër shih Surblyte, Gintare˙, Editor, *"Competition on the Internet"*, Vol. 23, Max Planck Institute for Innovation and Competition, Munich Germany, 2015.

se çështja e përdorimit të internetit do vijojë të *"torturojë"* institucionet e vendeve të ndryshme në lidhje me qasjet dhe mundësitë që jep interneti, pasi çështje si konkurrenca në treg, hapësira në internet apo siç njihen ndryshe domain[5] janë bërë shkak për diskutime dhe përlasjeve të shumta si brenda BE-së (ndërmjet vendeve anëtare) ashtu dhe jashtë saj, duke evidentuar dosmosdoshmërinë e përmirësimit të vazhdueshëm të legjislacionit të saj. Nuk duhet lënë pas dore investimi dhe puna jashtëzakonisht e madhe e bërë nga Organizata Botërore e Pronësisë Intelektuale *(WIPO – World Intelektual Property Organisation)* që ka në fokus mbrojtjen e krijimitarisë intelektuale. Kjo organizatë, në kuadër të zhvillimeve të reja, ka ndërtuar një rrjet komunikimi *"ndërkufitar"* për zgjidhjen e çështjeve të problematikave të shkeljeve të pretenduara të Pronësisë Intelektuale. Pikërisht kjo ndihmë dhe komunikim i ndërsjelltë dhe dhënia apo marrja e informacionit realizohet në mënyrë të shpejtë dhe pa kosto shtesë, kjo falë internetit. Por është pikërisht ky moment, që ashtu siç e letëson çështjen e komunikimit në kuadër të shkëmbimit të prodhimtarisë intelektuale ndërmjet bizneseve nga njëri vend në tjetrin, sjell edhe fenomene negative të abuzimit apo shkeljeve të të drejtave të autorëve të kësaj krijimtarie, duke cënuar të drejtat morale por edhe ekonomike të këtyre të fundit nga subjektet përfituese.

Shumë shtete kanë synuar që nëpërmjet parashikimeve në legjislacionet e tyre të parandalojnë situatat e abuzimit me krijimtarin intelektuale, me qëllim që ti mundësojë krijuesve që të ndihen jo vetëm të mbrojtur por edhe më produktiv në krijimtarinë e tyre, pikërisht për shkak të këtij ambienti të sigurtë. Në këtë kuadër mbrojtja që ofrohet është jo vetëm e aspektit civil dhe administrativ, por edhe e aspektit penal. Ky rregullim i karakterit penal në fushën e mbrojtjes së pronësisë intelektuale varion nga njëri vend në tjetrin.

Në kuadër të një integrimi tërësor të të gjitha fushave të shoqërisë edhe ajo shqiptare po ecën në këtë rrugë përmirësimi të vazhdueshëm të legjislacionit për mbrojtjen e të drejtave që burojnë nga aktiviteti dhe krijimtaria intelektuale. Kjo ka sjellë një sërë nismash legjislative të karakterit administrative/civil dhe njëkohësisht penal, të cilat kanë pasur si produkt final fokusin e mbrojtjes të krijimtarisë intelektuale. Nismat në fjalë janë pasuar nga nisma të tjera me qëllim përmirësimin e vazhdueshme të këtij kuadri legjislativ, për të qenë sa më i azhornuar dhe bashkëkohor me zhvillimet shoqërore në përgjithësi dhe ato të teknologjisë digjitale në veçanti.

5 Për më tepër për këtë çështje shih: Lipton, Jacqueline, "Internet Domain Names, Trademarks and Free Speech", Published by Edëard Elgar Publishing Limited, Cheltenham, UK • Northampton, MA, USA, 2010.

2. MBI ZHVILLIMIN E KUADRIT LIGJOR TË TË DREJTËS SË PRONËSISË INTELEKTUALE NË SHQIPËRI.

Përsa i përket çështjes së mbrojtjes të të drejtës së pronësisë intelektuale në Shqipëri, filloi të gjente një dismension të zgjeruar vetëm pas viteve '90. Pavarësisht kësaj edhe më parë ka pasur synim për rregullimin e saj qoftë para periudhës së monizmit qoftë gjatë periudhës kur u instalua sistemi monist në Shqipëri. Kështu rregullimin e të drejtës së pronësisë intelektuale mund të referojmë në rregullimin që bën Kodi Civil i vitit 1929, *"Neni 795. – Produktet intelektuale zotnohen prej auktorëve të tyne simbas rregullave të çaktueme në ligjat e posaçme."*[6] Kjo në kaudër të asaj çfarë përfaqësonte koha në kohën kur u hartua ky kod, periudhe në të cilën refletonte qëllimet për sjelljen e një fryme perëndimore në legjislacionin e ri shqiptar, kryesisht me referim në eksperiencat më të mira të kodeve civile të vendeve perëndimore si ai i Frances apo Italisë.Edhe pas instalimit të sistemit komunist në Shqipëri, rregullimi ligjor në mbrojtje të të drejtave të autorit nuk ka pasur një rregullim dhe fokus të mirëfilltë ashtu siç ndodhi pas viteve '90.

Kështu, në periudhën e monizmit, si një moment i dytë i zhvillimit të legjislacionit për mbrojtjen e të drejtës së pronësisë intelektuale, mund të flitet për miratimin e një kuadri ligjor ku mund të citojmë: Dekreti i Markave ne Prodhim dhe te Tregtise Nr. 2490, date 22.07.1957, ndryshuar me dekretet Nr. 3530, date 2.07.1962 dhe Nr.4253, date 11.04.196;[7] Kodi Civil i vitit 1981 në nenet 329 -335 te Kodit Civil ("E drejta e shpikjes dhe racionalizimit"), miratuar me Ligjin Nr.6340 date 26.06.1981 dhe 333(a) miratuar me Dekretin Nr. 7316 date 1989.

Pas viteve '90, me ndikimin edhe të faktorit ndërkombëtar, referuar rëndësisë së madhe që ka mbrojtja e pronësisë intelektuale, filloi një proces modernizimi dhe plotësimi të kuadrit ligjor. Këtu, si pjesë e kuadrit ligjor fillestar mund të përmendim ligjin nr. 7564, datë 19.05.1992 "Për të drejtën e autorit"; ligji nr.7819, datë 27.4.1994 "Për Pronësinë Industriale"; ligji Nr.8488, date 13.5.1999 "Për mbrojtjen e topografisë së qarqeve të integruara". Më pas, ky kuadër ligjor fillestar u shoqërua me përmirësime të vazhdueshem, duke miratuar ligjin nr. 9380, datë 28.4.2005 "Për të drejtën e autorit dhe të drejtat e tjera të lidhura me të" që aktualisht është shfuqizuaru me ligjin nr. 35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura

6 Kodi Civil – Mbretnia Shqiptare, shtypur nga shtypëshkronja albPaper, Tiranë, prill 2010, fq. 279.

7 Dhoma e Tregtisë dhe Industrisë luante rolin e përfaqësuesit të autorizuar të markave dhe patentave. Pranë kësaj zyre depozitoheshin markat dhe patentat.

me to" (i ndryshuar) ligj ky i përafruar me kuadrin ligjor rregullator të BE-së (direktivat); ligji nr. 9947, datë 07.07.2008 "Për Pronësinë Industriale". Gjithashtu, nuk duhen harruar dhe ratifikimi dhe bërja pjesë e legjislacionit të brendshëm, të një sërë konventash ndërkombëtare, që si fokus kanë rregullimin në fushën e pronësisë intelektuale. Këtu mund të përmendim miratimin e ligjit nr.10 179, datë 29.10.2009 "Për aderimin e Republikës së Shqipërisë në Konventën e Patentave Europiane"; ligjit nr.9950, datë 10.7.2008 "Për Aderimin e Republikës së Shqipërisë në ndryshimet e "Marrëveshjes së TRIPS-it (aspekte të tregtisë, që lidhen me pronësinë intelektuale)"; ligji nr. 9647, datë 27.11.2006 "Për aderimin e Republikës së Shqipërisë në aktin e Gjenevës të Marrëveshjes së Hagës për Regjistrimin Ndërkombëtar të Projekteve Industriale dhe rregulloret mbështetur në aktin e gjenevës, 1999"; ligji nr.9129 date 08.09.2003 "Për aderimin e Republikës së Shqipërisë në "Konventën Universale për të Drejtën e Autorit" dhe dy protokollet shtese te saj".

Nga kuadri ligjor sa prezantohet më sipër, evidentohet qartazi rëndësia që i është dhënë mbrojtjes së pronësisë intelektuale edhe në vendin tonë, mbrojtje që normalisht duhet të ishte shoqëruar me një impakt të rëndësishëm në zhvillimin ekonomiko-social brenda Shqipërisë. Në fakt realitet shqiptar prezantohet disi ndryshe, pasi është një fakt që duhet pranuar se niveli i shkeljes të të drejtës së pronësisë intelektuale tek ne është në një nivel jo pak të konsiderueshëm. Kjo situatë e ndikuar nga një sërë faktorësh ku mund të përmendim punën e organeve që objekt të punës së tyre kanë pikërisht administrimin dhe monitorimin e vazhdueshëm të aktivitetit në përgjithësi, në mbrojtje të këtyre të drejtave.

3. MBROJTJA NGA LEGJISLACIONI PENAL SHQIPTAR I TË DREJTAVE TË PRONËSISË INTELEKTUALE NË KUADËR TË AKTIVITETI NË INTERNET. BASHKËPUNIMI NË NIVEL NDËRKOMBËTAR.

Të drejtat e pronësisë intelektuale edhe në Shqipëri, si në shumë vende të tjera të rajonit por edhe më gjerë, bëjnë pjesë në kategorinë e të drejtave që mbrohet me Kushtetutën e SH-së. Kështu në nenin 41 të Kushtetutës parashikohet se *"1. E drejta e pronës private është e garantuar...."*[8] dhe në mënyrë më specifike këtë rregullim e gjejmë në nenin 58 të Kushtetutës parashikohet së: *"1. Liria e krijimit artistik dhe e kërkimit shkencor, vënia*

8 Kushtetuta e Republikës se Shqipërisë, Qëndra e Botimeve Zyrtare, Tiranë 2018.

në përdorim, si dhe përfitimi prej arritjeve të tyre janë të garantuara për të gjithë. 2. E drejta e autorit mbrohet me ligj."[9]

Duke qenë një çështje serioze me impakt domethënës në zhvillimin ekonomiko shoqëror në nivel kombëtar dhe ndërkombëtar, mbrojtja e pronësisë intelektuale është shoqëruar jo vetëm me kuadër rregullator të aspektit civilo-administrativ, ku mund të përmendim ligjin nr. 9947, datë 07.07.2008 "Për pronësinë Industriale" (i ndryshuar) apo ligjin 35/2016 "Për të drejtat e autorit dhe të drejtat e lidhura me të" (i ndryshuar) si dhe gjithë kuadrit rregullator, që parashikojnë rregullimin e kësaj fushe dhe organet kryesore përgjegjëse për monitorimin e respektimit të këtyre të drejtave, por edhe penale. Pikërisht mbrojtja e karakterit penale, duke bërë pjesë të Kodit Penale disa marrëdhënie të kësaj fushe, duke parashikuar përgjegjësinë penale për subjektet që shkelin këto të drejta është një tregues i rëndësishëm i synimit të çdo shteti dhe rastin konkret Shteti Shqiptar për ndëshkimin e çdo shkelje, duke synuar në sigurimin e një ambienti sa më të sigurtë zhvillimi.

Kodi Penal shqiptar parashikon dënimin e subjekteve që cënojnë apo shkelin të drejtat e sferës së pronësisë intelektuale, ku konkretisht mund të referojmë dispozitat si më poshtë:

- *Neni 148 - Botimit të veprës së tjetrit në emrin e vet;*
- *Neni 149 – Shkelja e të drejtave të autorit;*
- *Neni 149/a – Shkelja e të drejtave të pronësisë industrial;*
- *Neni 149/b - Shkelja e të drejtave të topografisë së qarkut të gjysmëpërçuesit.*

Përfshirja apo kualifikimi e një aktiviteti apo veprimtarie të tillë, ashtu siç dhe më sipër u përmend, evidenton rëndësinë e madhe që ka marrë domosdoshmëria e mbrojtjes së kësaj krijimtarie, në kuadër të zhvillimit normal të sektorëve me impakt në zhvillimin e shoqërisë.

Por, ashtu si më sipër u evidentua, fakti është se pavarësisht mbrojtjes së shumëfishtë që ofrohet, përsëri niveli i shkeljes së pronësisë intelektuale sidomos në drejtim të të drejtave të autorit por dhe të të drejtave të pronësisë industrial është shumë i lartë në vendin tonë, pavarësisht aktivitetit apo punës të këtyre organeve. Përsa i përket rasteve praktike, më shumë peshë specifike zënë çështjet gjyqësore të karakterit civilo-administrativ, ndërsa ato penale shumë më pak, kjo referuar situatës së përgjithshme në lidhje me çështjet e ndjekuara nga prokuroritë ndaj autorëve të pretenduar si shkelës të

9 Po aty.

të drejtave të pronësisë intelektuale. Kjo vjen për shumë arsye të cilat lidhen qoftë me mundësitë efektive të tyre, por edhe të çështjeve të karakaterit juridiksional, të kohës që ka kaluar nga momenti që evidentohet shkelja etj.. Pikërisht kjo përfaqëson dhe fokusin e pjesës në vijim të këtij punimi, duke sjellë në vëmendje të drejtat e pronësisë intelektuale në kuadër të shpërndarjes së informacionit në internet, në prizmin e përgjegjësisë penale në Shqipëri, ndaj subjekteve të pretenduara se kryejnë këto shkelje.

3.1 PRONËSIA INTELEKTUALE DHE AKTIVITETI NË INTERNET. BASHKËPUNIMI NË NIVEL NDËRKOMBËTAR.

Konkretizimi i mbrojtjes për pronësinë intelektuale është jo në një nivel të kënaqshëm. Kjo për faktin e shtrirjes së vazhdueshme të përdorimit të internetit në pothuajse të gjithë sektorët e ekonomisë dhe shoqërisë në përgjithës. Aplikimi i lidhjeve të ***"internetit"*** në shumicën e sektorëve, ka ofruar mundësi shumë të mira të shpërndarjes të të dhënave, informacionit, krjimtarisë etj. në rrjet në kohë shumë të shpejtë. Pavarësisht aspekteve pozitive të mundësive që ofron një përdorim kaq i zgjeruar i internetit në shumë sektorë, nuk duhen lënë pas dore aspektet negative të tij me pasojë cënimin e të drejtave të pronësisë intelektuale dhe jo vetëm.[10] Në kuadër të një procesi globalizimi të ekonomisë,[11] zhvillimi teknologjisë së komunikimit është primare për shkak edhe të lehtësirave që ofrohen në shpërndarjen e këtij informacioni dhe njëkohësisht me mundësinë për shmangien nga përgjegjësia në rastet e shkeljeve të pretenduara.[12] Prandaj çështja e mbrojtjes të të drejtave

10 Një aspekt shumë i rëndësishëm që duhet mbajtur në konsideratë është edhe çështja e përdorimit të të dhënave, që evidenton një trinom të një marrëdhënie që më shumë shoqërohet nga tensionet mes individëve, biznesit dhe qeverisë. Është një trinom subjektesh të përshira në këtë aktivitet, ku individët presin mbrojtje, bizneset rritjen e aktivitetit dhe qeveria nga e cila kërkohet rregullimi i marrëdhënies mes individëve dhe bizneseve por edhe mes këtij të fundit dhe qeverisë. Për më tepër mbi këtë çështje shih Bernal, Paul, *"Internet Privacy Rights - Rights to Protect Autonomy"*, University Printing House, Cambridge CB2 8BS, United Kingdom, 2014.

11 Për hirë të së vërtetës, çështja e procesit të globalizimit të ekonomisë u vu në diskutim dhe vijon të jetë pjesë e diskutimeve pas periudhës së pandemisë, me ndikim edhe çështja e luftës në Ukrahinë që pati jo pak impakt në ekonominë globale. Por sidomos periudha e pandemisë pati një ndikim të madh ndryshimi në qasjet e biznesit në tregjet përtej vendeve të origjinës. Mjafton të referojmë në rastin e kompanisë Apple në lidhje me politikat e saj të prodhimit të përçuesave dhe gjysëmpërçuesave që prodhoheshin në Kinë, kur u përball me një efekt të mungesës së tyre për shkak të një lockdoën-i që pati jo vetëm Kina, gjatë periudhë së pandemisë.

12 Mjafton të referojmë në një situatë aktuale në Shqipëri, ku në mënyrë më specifike do referojmë në çështjen e aktiviteteve në punimet shkencore në fushën akademike. Nuk kanë qenë të pakta rastet ku jemi hasur me situata ku subjekte të caktuara, përfshirë edhe një numër të konsiderueshëm të eksponentë të jetës politike në vend, janë gjetur me plagjatura në punimet e tyre shkencore. Pavarësisht denoncimeve me emër dhe mbiemër, jemi në një situatë që ndaj

që vinë nga krijimtaria intelektuale, merr një rëndësi të veçantë jo vetëm të karakterit kombëtar por dhe të një niveli ndërkombëtar me kërkesë për një bashkëpunim ndërinstitucional ndërmjet organeve ligjzbatuese të vendeve respektive apo dhe të krijimit të organizmave të përbashkët që operojnë në mbrojtje të këtyre të drejtave. Pavarësisht përpjekjeve në nivel jo më kombëtar, pavarësisht miratimin të legjislacionit në këtë drejtim e përafruar me direktivat e BE-së, përsëri mundësia për t'iu shmangur përgjegjësit civile dhe asaj penale nga subjektet shkelëse të ligjit është dhe vijon të jetë në nivel të lartë. Në këtë drejtim *(të evidentimit dhe dënimit të cënuesve)* gjykatat janë gjendur para situatave në të cilat janë detyruar të përfshihen në të edhe analiza në drejtim të evidentimin dhe përcaktimit të saktë të përgjegjësisë të autorëve të pretenduar. Kjo për vetë faktin se procesi i provueshmërisë së përgjegjësisë nga ana e autoriteteve të ndjekjes penale kërkon mbledhjen e provave, prova të cilat nuk janë lehtësisht të gjendshme për faktin e aftësive të mira në fshehjen e gjurmueshmërisë nga ana e autorëve të mundshme, sidomos kur kemi një situatë të aktivitetit që tejkalon kufinjtë fizik ndërmjet shteteve. Një punë e mirë në këtë drejtim është bërë me marrëveshjet në nivel ndërkombëtar, ku mund të përmendim marrëveshjen TRIPS (Marrëveshje tregtare të Aspektit të të Drejtave të Pronësisë Intelektuale / Trade Related Aspects of Intelectual Property Right), që edhe pse një marrëveshje që funksionon në kuadër të WTO (Organizatës Ndërmombëtare të Tregtisë/ World Trade Organisation), ka sjell një klimë përmirësimi për shkak të funksionimi në kohë reale dhe e pa kufizuar në aspektin e juridiksionit (kjo për shtetet nënshkruese të kësaj marrëveshje). Por pavarësisht, aktiviteti për gjurmimin dhe gjetjen e shkelësve të të drejtave të Pronësisë Intelektuale nërpërmjet internetit, kjo nuk është diçka gjithmonë e lehtë. Në këtë kuadër, referuar nenit 61 të marrëveshjes TRIPS, kërkohet juridiksioni i gjykatave që të mundësojë sekuestrimin dhe konfiskimin e *"çdo materiali…që është përdorur në kryerjen e veprës penale"*. Në këtë drejtim pyetja që lind është: *A mundet policia dhe prokuroria dhe më pas gjykata të kenë juridiksion për gjurmuar dhe kapur faqet e internetit apo emrat e domain që të cojnë në evidentimin e autorëve të mundshëm?* Ka vende që parashikojnë në legjislacionet e tyre një situatë të tillë, duke mundësuar sekuestrime domain si instrumente krimi apo si pronë duke iu nënshtruar konfiskimit. Shumë vende kanë qasje të ndryshme në këtë drejtim. Por nuk duhet mohuar fakti se marrëveshjet ndërkombëtare dhe organet ligjzbatuese me juridiksion

këtyre subjekteve nuk është ndërmarrë asnjë hap në drejtim të përgjegjësisë së tyre civile dhe jo më të mendohet të shkohet më tej drejt përgjegjësisë së tyre penale, pavarësisht se nga këto krijimtari intelektuale e të tjerëve, subjektet shkelëse kanë përfituar dhe vijojnë të përfitojnë pasi nuk është marrë asnjë masë qoftë administrative për heqjen e titujve shkencor që ata kanë marrë.

mbikombëtar kanë ndikuar në këtë drejtim.

Pikërisht ligji 35/2016 me referim në Konventën e Bernës ka ndihmuar në lehtësimin e punës së prokurorisë në provueshmërinë e akuzës, duke përfshirë prezumime si:

1. *Personi, emri i të cilit vendoset mbi vepër si autor i saj në mënyrë të zakonshme, supozohet se është autori i veprës.*
2. *Kur një pseudonym i përdorur nuk lë asnjë dyshim në identitetin e autorit, personi i treguar konsiderohet se është autori.*
3. *Në rastin e një vepre anonime ose me pseudonym, botuesi, emri i të cilit figuron në vepër, supozohet se përfaqëson autorin dhe me këtë aftësi do ketë të drejtë të ushtrojë dhe zbatojë të drejtat morale dhe ekonomike të autorit.etj.*

Pavarësisht kësaj duhet mbajtur në konsideratë që jemi në kushtet e situatës së qarkullimit "pakufinjë" (bordless) dhe pikërisht jemi në kushtet që kemi të bëjmë me situata ku autorët mund të ndodhen jashtë vendit. Prandaj organet ligjzbatuese të cilat kanë një juridiksion ndërkombëtar, siç është rasti i INTERPOL, EUROPOL etj. janë organe që mund të ndihmojnë në drejtim të gjurmimit, gjetjes dhe administrimit të këtyre provave për të vënë para drejtësisë shkelësit e këtyre të drejtave.

3.2 PARASHIKIMET NË KODIN PENALE SHQIPTAR DHE PËRMIRËSIMET E MUNDSHME.

Pavarësisht një bashkëpunimi të mirë ndërinstitucional me vendet e tjera, lë për të dëshiruar konkretizimi praktik në territorin tonë sidomos në drejtim të zbatimit dhe efektshmërisë së masave ndaj autorëve të mundshëm veprave penale të kësaj kategorie.

Duhet pranuar fakti se legjislacioni ynë nuk ***"shquhet"*** për masa të tilla të ashpra dhe nuk janë të krahasueshme me parashikimet në vende të tjera ku si referim mund të përmendim ashpërsinë me të cilën ndiqen dhe masat e dënimit të parashikuara në legjislacionin e SHBA-së. Ai parashikon veç masave ndëshkuese të karakterit administrativo-penal *(sic është rasti i gjobave të cilat janë në vlera të konsiderueshme apo konfiskimit të mjeteve që përdoren apo që parashikohen të përdoren për të kryer apo lehtësuar veprat penale)*, edhe masa të dënimit me burgim të cilat mund të shkojnë deri në dhjetë vite. Por pa pretenduar të arrijmë standartet e SHBA-së, e cila është një ndër promotorët dhe nxitëset e mbrojtjes së pronësisë intelektuale, duke e konsideruar një krim serioz cënimin e këtyre të drejtave, do të referojmë

në legjislacionin e Republikës së Kosovës, që në Kodin Penal parashikojnë marzhe dënimi shumë më të larta se në Kodin Penal të Republikës së Shqipërisë. Kështu në dispozitat që parashikojnë çështje të kësaj natyre, konkretisht **nenet 289 - Cenimi i të drejtave të patentës; nenin 290 - Cenimi i të drejtave të autorit; neni 291 - Shmangia e masave teknologjik** parashikohen, përveç masës së gjobave edhe marzhe dënimi me burg që shkojnë deri në pesë apo tetë vite.[13] Ndërsa, po të referojmë në parashikimet e Kodit Penal të Republikës së Shqipërisë, nuk përfshihen masa të tilla kaq të ashpra. Kështu në **nenin 148 - Botimi i veprës së tjetrit me emrin e vet**, parashikon se: *"Botimi ose përdorimi tërësisht apo pjesërisht me emrin e vet të një vepre letrare, muzikore, artistike ose shkencore që i përket një tjetri, përbën kundërvajtje penale dhe dënohet me gjobë ose **me burgim gjer në dy vjet**."*. Ndërsa në **nenin 149 - Shkelja e të drejtave të autorit** që parashikon se: *"Riprodhimi tërësisht ose pjesërisht, shpërndarja, komunikimi në publik, shitja, ofrimi për shitje, përdorimi, furnizimi, eksportimi ose importimi për qëllime fitimi i veprës së mbrojtur nga e drejta e 86 autorit, pa pëlqimin e autorit ose mbajtësit të së drejtës, kur janë shkelur të drejtat vetjake ose pasurore të tij, përbën kundërvajtje penale dhe **dënohet me gjobë ose me burgim deri në dy vjet.***

*Po kjo vepër, kur kryhet në bashkëpunim ose më shumë se një herë, **dënohet me burgim deri në tre vjet.**"* E njëjta situatë paraqitet edhe në **nenet 149/a - Shkelja e të drejtave të pronësisë industrial**, **149/b - Shkelja e të drejtave të topografisë së qarkut të gjysmëpërçuesit**, marzhet e masave të dënimit shkojnë nga gjoba deri në një maksimumi dy vite burgim.

Të tilla shkelje sipas legjislacionit tonë kanë ngelur në kuadër më shumë të natyrës së kundravajtjeve penale, referuar dhe marzheve në maksimumin e situatës më të rënduar *(në një apo tri vite)*. Prandaj, nuk mjafton gadishmëria për të bashkëpunuar në këtë drejtim me organet ligjzbatuese të vendeve të tjera, apo përafrimi që i bëhet legjislacionit, kur ndaj shkelësve parashikohet masa të tilla kaq të zbutura dënimi. Kjo në një farë mënyrë zbeh këto nisma ligjore dhe njëkohësisht punën dhe interesin për të imponuar respektimin

13 Në Kodin Penal të Republikës së Kosovës masa e dënimit me burgim lidhet dhe me masën e përfitimit nga ana e autorit të veprës penale. Pikërisht kjo është më e përshtatshme se parashikimet përgjithsësuese që bën legjislacioni ynë penal. Kështu në nenin 290 parashikohet se: *"...6. Nëse gjatë kryerjes së veprës penale nga paragrafi 5. i këtij neni, kryesi ka përfituar për vete ose për personin tjetër së paku dhjetë mijë (10.000) Euro por më pak se pesëdhjetëmijë (50.000) Euro, kryesi dënohet me gjobë dhe me burgim prej tre (3) muaj deri në pesë (5) vjet. 7. Nëse kryesi i veprës penale nga paragrafi 5. i këtij neni përfiton për vete ose për personin tjetër më shumë se pesëdhjetëmijë (50.000) Euro, kryesi dënohet me gjobë dhe me burgim prej gjashtë (6) muaj deri në tetë (8) vjet..."* - KODI NR. 06/L-074 KODI PENAL I REPUBLIKËS SË KOSOVËS - GAZETA ZYRTARE E REPUBLIKËS SË KOSOVËS / Nr. 2 / 14 JANAR 2019, PRISHTINË.

dhe për të treguar nivelin e seriozitetit në mbrojtje të të drejtave të pronësisë intelektuale.

Përveç faktit të mësipërm, nuk duhet lënë pas dore edhe çështja e afateve kohore nga momenti i konstatimit të veprimeve penalisht të dënueshme dhe fillimit të veprës penale. Mund të hasen vështirësi procedurale që lidhen me pamundësinë e ushtrimit të ndjekjes për shkak të parashkrimit ***(nenit 66 - Parashkrimi i ndjekjes penale të K.Penal)***. Kjo, sjell mosndëshkueshmërinë e autorëve të veprave penale të kësaj kategorie, pa përmendur këtu dhe ndryshimet ndërmjet legjislacioneve penale nga njëri vend tek tjetri përsa i përket masave të dënimit, ku mbi bazën e instrumenteve procedural mund të arrihet shmangie të dënimeve nga legjislacionet që kanë marzhe dënimi të larta. Në këtë kuadër, puna e organeve të procedimit penale duhet të jetë e atij niveli që të mundësojë ndjekjen penale dhe dënimin e këtyre subjekteve dhe të pamunësojë hapësirat që synojnë të shfrytëzojnë këta të fundit.

Duke qenë se vepra penale që lidhen me të drejtën e pronësisë intelektuale qoftë nga procedime të deri tanishme por edhe nga mënyra se si ato kryhen, kanë të bëjnë me përdorimin e paisjeve kompjuterike apo metodave të tjera siç mund të jetë mashtrimi, fshehja e të ardhurave nga ky aktivitet, ndërhyrjet në të dhënat kompjuterike etj.[14] Pikërisht në këtë prizëm, përfshirja gjatë hetimeve edhe të akuzave të tjera, bazuar pikërisht në këto dispozita të Kodit Penal që shihen të lidhura ngushtësisht *(kjo e hetuar rast pas rasti)* me procedimet penale për shkeljen e të drejtave të autorit apo të drejtave industriale, bëjnë që pozita e personave të akuzuar të rëndohet akoma më shumë, duke e bërë të mundur një ndëshkim të tyre.

Ndjekja penale ndaj shkelësve, kryesisht bazohet mbi bazën e kallëzimeve që vinë nga subjektet që kanë detyrë monitorimin apo subjekteve që preken drejtpërdrejtë nga vepra penale. Pikërisht, duke referuar subjekteve që kanë si fokus të punës së tyre mbrotjen nga shkelje të të drejtave të pronësisë intelektuale në internet, mund të referojmë rastin e Autoritetit të Komunikimit Elektronik dhe Postar (AKEP), që përfaqëson një person juridik publik jo buxhetor. Ky autoritet menaxhon veprimtarin e hyrjeve dhe publikimeve të ëebsite-ve në internet, nëpërmjet IP (protokolleve në

14 Kodi Penal i Republikës së Shqipërisë parashikon një sërë veprash që lidhen pikërisht me informacionin, të dhënat etj. me përdorimin e internetit duke përdorur paisjet kompjuterike. Kështu, mund të referojmë dispozitat në Kodin Penal që gjatë hetimeve mund të shihen të lidhura me veprën penale të shkeljes të të drejtave të pronësisë intelektuale ku mund të përmendim: neni 143/b - Mashtrimi kompjuterik; neni 180 – Fshehja e të ardhurave; neni 186/a - Falsifikimi kompjuterik; neni 192/b - Hyrja e paautorizuar kompjuterike; neni 293/b - Ndërhyrja në të dhënat kompjuterike; neni 293/c - Ndërhyrja në sistemet kompjuterike; Neni 293/ç - Keqpërdorimi i pajisjeve.

internet). Ky organ publik nëpërmjet platformave të liçensuara nga shoqëri të ndryshme që kanë kuadër shpëndarje në internet si p.sh ACROMAX Ltd., një shoqëri me seli në Izrael, ushtron aktivitetin e kontrollit dhe bllokimit të të gjithë postimeve apo punëve të shpëndara në internet, që nuk referojnë burimin apo që konstatohen në shkelje të këtyre të drejtave. Nga ky aktivitet, AKEP-i vihet në dijeni të kryerjes së një vepre penale të kësaj kategorie dhe ka detyrimin që të bëj kallëzimet përkatëse penale pranë organit të ndjekjes penale. Pikërisht iniciativa të tillë janë shumë të rradha për të mos thënë inekzistente, ç'ka evidenton domosdoshmërinë e ndryshimit të qëndrimeve dhe ndërgjegjësimin, jo vetëm të këtij subjekti por të të gjithë subjekteve fizik apo juridik, të cilët vihen në dijeni për shkelje të tilla.

Në përfundim, duam të vëmë në dukje se sa u trajtua më sipër, me qëllim ndëshkimin duke synuar ndërgjegjësimin e publikut të gjerë në drejtim të rëndësisë që ka mbrojtja e të drejtave të pronësisë intelektuale me impakt ekonomiko-social në shoqërinë tonë, rekomandohet si domosdoshmëri:

- Rritja e ndërgjegjësimit të organeve që kanë në fokus mbrojtjen e këtyre të drejtave,

  duke synuar rritjen e nivelit të kërkesës së llogarisë ndaj aktivitetit të tyre;

- Përmirësimi i kuadrit ligjor penal, duke shkuar drejt një *"ashpërsimi"* të masave të

  dënimeve të dispozitave të parashikuara në Kodin Penal të Republikës së Shqipërisë, që synojnë mbrojtjen e të drejtave të pronësisë intelektuale *(të drejtave të autorit dhe të drejtat e lidhur me të si dhe të drejtave të pronësisë industriale)*.

- Njëkohësisht rekomandohet që ndjekja penale në raste të tilla, nga ana e organeve

  të procedimit penale, që evidentohet në shkelje të këtyre të drejtave referohet sëbashku me parashikime të tjera të lidhura edhe me vepra të tjera penale, ç'ka ndikon në mundësinë e arritjes së një ndëshkimi dhe njëkohësisht ndërgjegjësimi më të mirë të publikut të gjerë.

LITERATURA E KONSULTUAR

Botime dhe artikuj

- Surblyte, Gintare˙, Editor, "Competition on the Internet", Vol. 23, Max Planck Institute for Innovation and Competition, Munich Germany, 2015.
- Bernal, Paul, "Internet Privacy Rights - Rights to Protect Autonomy", University Printing House, Cambridge CB2 8BS, United Kingdom, 2014
- Lipton, Jacqueline, "Internet Domain Names, Trademarks and Free Speech", Published by Edward Elgar Publishing Limited, Cheltenham, UK • Northampton, MA, USA, 2010.
- Herrington K., TyAnna, "Controlling Voices - Intellectual Property, Humanistic Studies, and the Internet", Printed in the United States of America, 2001

Legjislacion

1. Kushtetuta e Republikes se Shqipërisë, Qëndra e Botimeve Zyrtare, Tiranë 2018.

2. Kodi Civil – Mbretnia Shqiptare, shtypur nga shtypëshkronja albPaper, Tiranë, prill 2010.

3. Kodi Penal i Republikës së Shqipërisë, botim i Qendrës së Botimeve Zyrtare, Tiranë 2019.

4. Dekreti i Markave ne Prodhim dhe te Tregtise Nr. 2490, date 22.07.1957 (ndryshuar me dekretet Nr. 3530, date 2.07.1962 dhe Nr.4253, date 11.04.196)

5. Kodi Civil i vitit 1981, miratuar me Ligjin Nr.6340 date 26.06.1981.

6. Ligji nr. 7564, datë 19.05.1992 "Për të drejtën e autorit";

7. Ligji nr.7819, datë 27.4.1994 "Për Pronësinë Industriale";

8. Ligji Nr.8488, date 13.5.1999 "Për mbrojtjen e topografisë së qarqeve të integruara"

9. Ligji nr. 9380, datë 28.4.2005 "Për të drejtën e autorit dhe të drejtat e tjera të lidhura me të" (i shfuqizuar)

10. Ligji nr. 35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to" (i ndryshuar)

11. Ligji nr. 9947, datë 07.07.2008 "Për Pronësinë Industriale"

12. Kodi nr. 06/L-074 Kodi Penal i Republikës së Kosovës - GAZETA ZYRTARE E REPUBLIKËS SË KOSOVËS / Nr. 2 / 14 JANAR 2019, PRISHTINË.

13. Ligjit nr.10 179, datë 29.10.2009 "Për aderimin e Republikës së Shqipërisë në Konventën e Patentave Europiane";

14. Ligji nr.9950, datë 10.7.2008 "Për Aderimin e Republikës së Shqipërisë në ndryshimet e "Marrëveshjes së TRIPS-it (aspekte të tregtisë, që lidhen me pronësinë intelektuale)".

15. Ligji nr.9647, datë 27.11.2006 "Për aderimin e Republikës së Shqipërisë në aktin e Gjenevës të Marrëveshjes së Hagës për Regjistrimin Ndërkombëtar të Projekteve Industriale dhe rregulloret mbështetur në aktin e gjenevës, 1999".

16. Ligji nr.9129 date 08.09.2003 "Për aderimin e Republikës së Shqipërisë në "Konventën Universale për të Drejtën e Autorit" dhe dy protokollet shtese te saj".

Faqe internet (website):

1. https://www.wipo.int konsulutar në datë 20.06.2022.

2. https://qbz.gov.al konsulutar në datat 10.07.2021.

3. https://https://gzk.rks-gov.net konsulutar në datat 12.07.2022.

PROTECTION OF PRIVATE LIFE FROM CRIMINAL OFFENSES CAUSED BY TECHNOLOGICAL DEVELOPMENTS

M.SC. ELJONA RUÇI

Abstract

The century we are living in, is considered the golden age of technology, where technological tools are advancing more and more every day and where each of the human beings is being influenced by becoming more and more dependent on this development. Even artificial intelligence is one of the types of technology development which is making it possible for the computer to have the ability to act as a human being.

Nowadays, technology is our tool of information, pleasure, entertainment, safety and health, so we can practically say that it covers all the most important spheres of life. However, this bright future unfortunately has a cost and in fact, more or less preserving privacy is coming to an end. This rapid and sophisticated development of technology is posing a difficult problem for humanity where there is increasingly the possibility that artificial intelligence can defeat man.

Based on the above conclusions, in every legal state there should be the sanctioning of criminal legal norms to effectively guarantee the recognition, development and protection of the various aspects in which the concept of private life materializes. And not only that!

This article will specifically address and analyze the various ways and forms of how legally developed technological tools affect the violation of privacy. Also, during this paper will be suggested preventive measures to reduce as much as possible criminal offenses that violate the private life of

the individual. These not only highlighting the improvement, change and supplementation of Albanian and European legislation, but also suggesting the avoidance of criminal offenses from technological impact through the practical implementation of alternative methods to reduce and curb this global phenomenon.

Key words: *technological tools, private life, artificial intelligence, criminal legal norms, preventive measures*

MBROJTJA E JETËS PRIVATE SI PASOJË E VEPRAVE PENALE TË SHKAKTUARA NGA ZHVILLIMET TEKNOLOGJIKE

M.Sc. Eljona Ruçi

Abstrakt

Shekulli ku po jetojmë konsiderohet si shekulli i artë i teknologjisë, ku mjetet teknologjike çdo ditë e më shumë po avancohen dhe ku secili prej qënieve njerëzore po ndikohet duke u bërë gjithmonë e më i varur nga ky zhvillim. Edhe inteligjenca artificiale është një ndër llojet e zhvillimit të teknologjisë e cila po bën të mundur që kompjuteri të ketë aftësinë që të veprojë si qënie njerëzore.

Në ditët e sotme, teknologjia është mjeti ynë i informacionit, i kënaqësise, i argëtimit, i sigurisë, dhe i shëndetit, pra praktikisht mund të themi se mbulon të gjitha sferat më të rëndësishme të jetës. Megjithatë, kjo e ardhme kaq e ndritur fatkeqësisht e ka një kosto dhe në fakt, pak a shumë ruajtjes së jetës private po i vjen fundi. Ky zhvillim kaq i shpejtë dhe i sofistikuar i teknologjisë po paraqet një problem të vështirë për njerëzimin ku ekziston gjithmonë e më shumë mundësia që inteligjenca artificiale ta mposhtë njeriun. Bazuar ne konkluzionet e mësipërme, në çdo shtet ligjor duhet të ekzistojë sanksionimi i normave juridiko - penale për të garantuar efektivisht njohjen, zhvillimin dhe mbrojtjen e aspekteve të ndryshme në të cilat materializohet koncepti i jetës private. Dhe jo vetëm kaq!

Në këtë artikull do të trajtohen e analizohen specifikisht mënyrat dhe format e ndryshme sesi ndikojnë ligjërisht mjetet e zhvilluara teknologjike në cënimin e jetës private. Gjithashtu, gjatë këtij punimi do të sugjerohen masat parandaluese për reduktimin sa më tepër të veprave penale qeë cënojnë jetën private të individit. Këto jo vetëm duke evidentuar përmirësimin, ndryshimin dhe plotësimin e legjislacionit shqiptar dhe atij europian, por edhe duke sugjeruar shmangien e veprave penale nga ndikimi teknologjik ndërmjet zbatimit në praktikë të metodave alternative për të reduktuar dhe frenuar sa më tepër këtë fenomen global.

Fjalët kyçe: *mjete teknologjike, jetë private, inteligjenca artificiale, norma penale juridike, masa parandaluese*

Hyrje

Të drejtat e njeriut e kanë prejardhjen rreth 2500 vjet më parë në filozofinë greke ndërmjet ndërthurjes së nocioneve të ligjit dhe drejtësisë natyrore, të lidhura këto ngushtësisht me njëra - tjetrën, por që nuk promovojnë ide të njëjta. Kjo pasi e drejta natyrore i përgjigjet ideve të ndërgjegjes/koshiencës dhe nevojës për drejtësi; ajo është subjektive dhe ndryshon nga njëri person, shoqëri dhe gjeneratë tek tjetra. Ndërsa e drejta ligjore gjendet tek rregullat e vendosura nga shtete të ndryshme, apo kur këto rregulla e norma vendosen nga drejtuesit e instancave mbi juridiksionet e tyre dhe rrjedhin nga pozitivizmi ligjor, që nënkuptohet këtu se ligjet e rregullat vendosen nga personat që kanë autoritetin për të drejtuar të tjerët, shpeshherë këta të fundit të vendosur në pozita inferioriteti të gjendur përballë këtyre instancave drejtuese.

Mund të thuhet se e drejta e respektimit të jetës private si një ndër të drejtat themelore të njeriut, përfaqësojnë një interpretim modern dhe një zgjerim të konceptit tradicional të "shtetit të së drejtës". Aktualisht, shkolla të ndryshme të së drejtës japin pikpamje kontradiktore lidhur me origjinën e moscënimit të jetës private, por ajo që vlen të përmendet është se një trup i të drejtave bazë ka ekzistuar që nga fundi i shek. të XVIII - të në Europë dhe ka qenë temë diskutimesh e debatesh që nga ajo periudhë në shkollat europiane të mendimit. Më konkretisht këto ide filluan të zhvilloheshin (kuptohet jo në mënyrën normale ligjore që njeh sot jurisprudenca moderne), në shekullin XIX - të me përfaqësues të spikatur si: Jeremy Bentham, John Austin, John Stuart Mill dhe në shekullin e XX – të koncepti për drejtësinë dhe lirinë individuale u zhvillua më tej nga filozofi John Rawls.[1]

Ato çfarë në ditët e sotme quhen të drejtat e njeriut, konsideroheshin më

përpara si të drejta natyrore dhe lindën si pasojë e nevojës së njeriut për të shpjeguar vendin e tij në univers. Me kalimin e kohës teoria e ligjit natyror u përpunua dhe u bë më e sofistikuar, duke patur si tendencë të krijohej mbi pikëpamje monoteiste/monopolizuese për jetën, por megjithatë prapë duke përmbajtur shumë pak parime në krahasim me evoluimin që ka arritur në kohët moderne.

Por, praktika ligjore e kohëve të sotme kërkon të njohë më tepër se kaq; për të pasur vendime gjykatash, si dhe zbatime praktike efektive dhe mbi të gjitha të drejta, duhet të nxisim arsyetimin se nëse e drejta për të pasur një jetë private të garantuar nga moscënimi i autoriteteve të ndryshme, duhet të konsiderohet në thelb si një e drejtë morale apo ligjore.

Tashmë, bazuar në këtë përqasje moderne të epokës që po jetojmë, është vendosur theksi më së shumti në të drejtat e njeriut se sa në të drejtat natyrore, duke u shtuar në këtë mënyrë edhe lista e të drejtave të individit, ku midis të tjerave është edhe garantimi për një jetë të qetë private, duke evoluar gjithmonë e në përmirësim të vazhdueshëm.

Në teorinë që arsyeton jurisprudenca ndërkombëtare ndryshimi konsiderohet i thjeshte. Sipas saj, të drejtat ligjore ekzistojnë në sistemet ligjore të cilat zbatohen brenda shtetit dhe midis vetë shteteve, por vetëm kur ato detyrohen nga traktate ose detyrime ndërkombëtare ligjore. Ndërkaq, të drejtat morale përshkruhen më së miri si pretendime morale, por ato nuk janë të sanksionuara diku, e si të tilla nuk mbrohen me ligj nga asnjë prej sistemeve ligjore.

Nëse e drejta për respektimin e jetës private pranohet se është një e drejtë objektive, ka përparësi të madhe dhe është një e drejtë universale, është e vetëkuptueshme se zbatimi i saj është i detyrueshëm dhe konkluzioni që mund të nxirret prej sa më sipër, është se kjo e drejtë është me prejardhje morale.

Megjithatë, nëse e drejta për respektimin e jetës private si një e drejtë e garantuar me ligj, është në varësi të ndyshimeve dhe shijeve kulturore, atëherë zbatimi universal nuk do të aplikohet për të dhe rezultatet që do ndikonin në praktikën ligjore do të bazohen në rregullat ligjore të gjendura brenda një juridiksioni të veçantë.

Si përfundim, nxjerrë nga teoritë si më sipër, vlen të pohohet se detyrimet morale qëndrojnë në thelbin e vendosjes së drejtësisë, ashtu sikurse praktika ligjore na ka sjellë plot shembuj që na bindin për vërtetësinë e këtij pohimi. Gjithashtu, në pratikë, jo vetëm e drejta për moscënimin e privatësisë, por të

gjitha dispozitat që përmbajnë të drejtat e njeriut janë hartuar që të zbatohen në sferat morale dhe ligjore, megjithëse shumica e tyre vendosen me detyrim nga ligji.

Një tjetër debat që është zhvilluar historikisht midis shkollave të ndryshme të së drejtës, ka të bëjë me faktin se nisur nga një analizë kontrastuese apo krahasuese, nëse e drejta për mbrojtjen e jetës private do të konsiderohet si një e drejtë universale apo relative.

Teoria Universale e të drejtave të njeriut parashtron idenë se ekziston një model ndërkombëtar i cili merr rëndësi dhe garanci ligjore kur përdoret në mënyrë uniforme në të gjithë botën. Pikërisht kjo është edhe teoria ku gjen mbështetje Deklarata Universale e Kombeve të Bashkuara, ku së bashku me dy Konventat ndërkombëtare binjake përbëjnë atë instrument të famshëm ligjor që njihet gjerësisht si Karta Ndërkombëtare e të Drejtave të Njeriut/ International Bill of Human Rights.[2]

Relativiteti kulturor është argumenti kundërshtues që manifeston teorinë se të drejtat e njeriut, disa prej të cilave mund të jenë të dëshirueshme por jo themelore, nuk janë uniforme apo domosdoshmërisht të bazuara në të drejtat civile e politike të individit dhe variojnë në sisteme të ndryshme ndërkombëtare në bazë të kulturave të ndryshme dhe të realitetit të ekzistencës së ndryshimeve të mëdha të zhvillimeve ekonomike dhe sociale në kontinente, vende dhe shoqëri të ndryshme.

Nëse do të ndaleshim tek mangësitë që shoqërojnë të drejtat e njeriut, vihet re se si dobësi themelore e relativitetit kulturor është se ajo shpesh herë përdoret në mënyrë arbitrare nga pushtetarë e zyrtarë në pozita pushteti, kryesisht në ato shtete ku popujt e tyre nuk kanë mundësi që të shprehin lirshëm mendimet dhe pikëpamjet e tyre rreth të drejtave dhe lirive të tyre, e kryesisht mbi moscënimin e privatësisë.

Ndërsa, si një këndvështrim negativ i argumentit universal ka të bëjë me faktin e pashmangshëm se, e drejta për respektimin e një jete private si një ndër të drejtat themelore e më të rëndësishme të njeriut nuk zbatohet, nuk vërehet dhe nuk respektohet në mënyrë universale përkundrejt asaj

- Calvo, C. (1885), Le Droit International, 5th ed Paris, (përkthyer nga origjinali në gjuhën spanjolle, Derecho international teorico and practico, 1868, Paris)
- Root, E., (1930), The basis of protection of citizens residing abroad, American Journal of International Law, No.24 se çfarë promovon teoria universale, pavarësisht se kjo e drejtë konsiderohet si një e drejtë e dhënë nga Zoti (ose forca të tjera universale) që i atribohet qënies

njerëzore që në momentin e konceptimit të tij/saj dhe që e shoqëron më pas përgjatë gjithë ekzistencës universale.

1. Roli i së Drejtës Ndërkombëtare në njohjen dhe sanksionimin e të drejtave e lirive të njeriut

Sikurse u trajtua më gjerësisht në hyrje të këtij punimi, disa prej mendimtarëve dhe filozofëve europianë më në emër të shekujve 18 dhe 19 zhvilluan dhe u fokusuan në konceptin e një grupi të drejtash të etiketuara ″të drejta natyrore″, si një trup të drejtash që kanë privilegjin ti gëzojnë të gjitha qëniet humane. Shumë nga këto të drejta u ligjëruan rreth shekullit të XVIII - të, ku shtete të tilla si Franca dhe Shtetet e Bashkuara të Amerikës miratuan respektivisht deklarata mbi të drejtat në kohën e krijimit të Republikës së parë të Francës pas revolucionit të vitit 1789 dhe në kohën e deklarimit të pavarësisë së ish kolonive britanike të Amerikës së Veriut.

Deklarata Franceze e të Drejtave të Njeriut (shpallur më 1789) dhe Deklarata e Pavarësisë së Shteteve të Bashkuara të Amerikës (shpallur më 1776), së bashku edhe me Kartën e të Drejtave/Bill of Rights (ku dhjetë amendamentet e para u ratifikuan në dhjetor të 1791) formuluan natyra të ndryshme të drejtash, përfshirë këtu të drejtën e lirisë dhe barazisë (duke nënkuptuar në këtë mënyrë edhe disa liri për jetesën personale), për tu gëzuar nga të gjithë shtetasit.

Karta Amerikane e të Drejtave[3] i referohet kryesisht lirisë së besimit (sanksionuar në Amendamentin I), kërkesave të ndryshme që lidhen me një proces të rregullt gjyqësor, si dhe të së drejtës që çdo qytetar gëzon për të pasur një gjykim të drejtë. Gjithashtu, në këtë Kartë përmbahen klauzola ligjzbatuese që kanë të bëjnë për një jetesë të lirë të individit, si dhe me lirinë e pronësisë për të gjithë shtetasit.

E rëndësishme këtu vlen të pohohet se të gjitha të drejtat e përmendura në paragrafin e mësipërm: janë sinkrone moderne në instrumentet që kanë zhvilluar të drejtat dhe lirive themelore të njeriut, si dhe përbëjnë bazën ku mbështetet Kushtetuta e ditëve të sotme e SHBA – ve që zbatohet nga gjykatat kombëtare.

Deklarata Franceze[4] fillon duke shprehur se *″Njerëzit lindin dhe mbeten të lirë dhe të barabartë në të drejta″*, ndërsa në nenin 4 të saj gjendet sanksionimi që i bëhet përkufizimit të konceptit të lirisë. Ndërkaq nene të tjera konsistojnë në ushtrimin e traditës së shtetit të së drejtës, duke përfshirë këtu edhe të drejtën për një proces të drejtë gjyqësor.

Kjo deklaratë për shkak të impaktit dhe rëndësisë së madhe që pati në shtetin e Francës shërbeu si bazë për Kushtetutat e mëvonshme franceze, përfshirë këtu edhe versionin e fundit të saj të vitit 1958. Gjithashtu, ndikimi i saj nuk u kufizua vetëm me hovin që pati në Francë, pasi

www.gpoaccess.gpo.gov/coredocs - Zyra e printimit të Qeverisë së Shteteve të Bashkuara të Amerikës

www.elysee.fr/ang/instit/text1.htm - Zyra e Presidentit Francez

deklarata franceze shërbeu si një udhërrefyes edhe për Kushtetutat e shteteve të tjera të Europës, për ish vendet e kolonizuara, sikundër edhe për vetë Konventën Europiane të të Drejtave të Njeriut.

1.1 Drejt mbrojtjes ndërkombëtare të të drejtave dhe lirive themelore të njeriut

Fillimisht e drejta ndërkombëtare nënkuptonte në të vërtetë të drejtën e shteteve/kombeve dhe kishte si qëllim të rregullonte marrëdhëniet midis shteteve: ligjet e luftës dhe marrëdhëniet diplomatike mes tyre. Deri relativisht vonë trajtimi që i bënin shtetet shtetasve të tyre ishte kompetencë ekskluzive e tyre. Pra, nga kjo lihet të kuptohet se mënyra e trajtimit nuk i nënshtrohej as rregullimit ndërkombëtar dhe as as rishikimeve nga jashtë.

Në vitet që pasuan luftërat e mëdha botërore u vu re se parimet origjinale me karakter humanitar jo rrallë herë injoroheshin dhe mënjanoheshin me vullnetin e ″palës sunduese″, duke cënuar shpeshherë haptazi të drejtën për një jetë private.

Problemet e zhurmshme e të njëpasnjëshme që po përjetonin popujt e Europës gjatë gjithë kësaj periudhe u bënë shkaktare për nxitjen e "ndryshimit të kursit" në rendin botëror. Në këto kushte ku gjendeshin shoqëritë botërore, nëse si synim të deklaruar kishin hemogjenitetin kombëtar, rezultati në realitet ishte kaosi në promovimin e lirive të individit.

Kësisoj, çështjet që kishin të bënin me mbrojtjen e minoriteteve dhe mbrojtjen sektoriale, të cilat ishin problemet kryesore ku po fokusoheshin autoritetet kombëtare gjatë dhe pas periudhës së dy luftërave botërore, tashmë filluan dalëngadalë të zëvendësoheshin nga përpjekjet e përbashkëta ndërkombëtare për të siguruar të drejtat dhe liritë themelore për të gjithë, pa diskriminim.

Menjëherë pas përfundimit të Lufës së Dytë Botërore u ngritën Organizata e Kombeve të Bashkuara dhe Këshilli i Europës, instrumente ndërkombëtare

të cilat vlerëson në ditët e sotme moderne për sistemet e tyre të zhvilluara në promovimin dhe mbojtjen e të drejtave të njeriut, e kryesisht për respektimin e të drejtës për një jetë private.

Vlen të theksohet se në periudhën përpara themelimit të Kombeve të Bashkuara mbrojtja dhe respektimi i të drejtave të njeriut ishte thjesht sporadike. Ndërkohë që ishin identifikuar tematikat e posaçme nga fuqitë dominuese politike dhe ekonomike të kohës, kërkoheshin edhe zgjidhje për trajtimin e tyre.

Në këtë mënyrë, duke marrë shkak nga problematikat për trajtimin e minoriteteve të veçanta, krahas krijimit të traktateve që krijuan kushtet e përshtatshme për mbrojtjen dhe repektimin e këtyre pakicave të veçanata për shtetet e interesuara (duke adresuar problematikat e këtyre grupeve vunerable të shoqërive të asaj periudhe), u pa e domosdoshme në praktikë krijimi i mekanizmave kontrollues ligjzbatues në nivel ndërkombëtar për të siguruar efektshmëri konkrete të traktateve të tilla.

Por, mbërritja e një mekanizmi të vërtetë ndërkombëtar, e krijuar nën petkun e abuzimeve në masë të këtyre të drejtave dhe shkeljeve haptazi të çështjeve që kishin në tematikë respektimin e jetës private, si edhe dalja në pah e vuajtjeve të përditshme katastrofike njerëzore, dalëngadalë siguroi kushtet e përshtatshme, në momentin e duhur, për krijimin e një platforme globale për lançimin dhe promovimin e të drejtave bashkëkohore të njeriut.

Kjo solli evoluimin me shpejtësi të sofistikimit të mbrojtjes së jetës private, duke mundësuar faktin që aktualisht, në ditët e sotme, një pjesë e konsiderueshme dhe e rëndësishme e së drejtës ndërkombëtare njeh dhe vlerëson të drejtat universale të njeriut.

2. Mekanizmat dhe institucionet ndërkombëtare që sigurojnë mbrojtjen dhe promovimin e repektimit të jetës private

2.1 Instrumentet ligjore të Kombeve të Bashkuara për mbrojtjen dhe promovimin e të drejtës për respektimin e jetës private, si një ndër të drejtat themelore të njeriut

Nëse do të bënim një rezume tepër përmbledhëse të instrumenteve ndërkombëtarë që kanë vepruar dhe vazhdojnë të shtrijnë ndikimin e tyre

edhe aktualisht në mbrojtjen dhe promovimin e të drejtave të njeriut, do të veçonim si momente kryesore këto ngjarje historike, kronologjikisht të klasifikuara si më poshtë vijon:

- Në vitin 1945 – Me krijimin e Kartës së Kombeve të Bashkuara u vendosën "rregullat e klubit"
- Në vitin 1948 – Në Deklaratën Universale të të Drejtave të Njeriut/ UDHR u shprehën aspiratat jodetyruese
- Në vitin 1966 – U miratuan dy mekanizma ndërkombëtare: Pakti Ndërkombëtar për të Drejtat Ekonomike, Sociale dhe Kulturore/ ICESCR, si dhe Pakti Ndërkombëtar për të Drejtat Civile dhe Politike/ICCPR
- Në vitin 1976 – Paktet hynë në fuqi, ku së bashku me Deklaratën Universale të të Drejtave të Njeriut, formuan atë mekanizëm global që njihet si Karta Ndërkombëtare e të Drejtave të Njeriut

2.1.1 Karta e Kombeve të Bashkuara

U bënë propozime për të përfshirë në Kartën e Kombeve të Bashkuara një paketë të drejtash, por kjo nuk u realizua për dy arsye kryesore:

- Së pari, Komisioni i Kombeve të Bashkuara për të Drejtat e Njeriut u themelua në vitin 1946
- Së dyti, në nenin 68 të saj parashikohej shprehimisht se Këshilli Ekonomik dhe Social/ECOSOC duhet të ngrinte komisione në fushat ekonomike dhe sociale për të bërë të mundur në praktikë nxitjen e zbatimit të së drejtave të njeriut

Që në parathënien e këtij instrumenti ndërkombëtar, më konkretisht në paragrafin e dytë, përveç të tjerave, i kushtohet rëndësi faktit që "*shtetet pjesëmarrëse në Organizatën e Kombeve të Bashkuara janë të vendosura të ripohojnë besimin në të drejtat themelore, si dhe në dinjitetin dhe vlerat e qenies njerëzore",* duke garantuar në këtë mënyrë vlerat universale që gëzon mbrojtja e jetës private nga cënime të ndryshme, si një ndër të drejtat themelore më të rëndësishme për një individ, në lëmin e morisë së të drejtave të njeriut.

Kjo kartë e vendos autoritetin e tij ligjzbatues ndërmjet këtyre veprimeve:

- I mundëson Këshillit Ekonomik dhe Social të Kombeve të Bashkuara bërjen e rekomandimeve për nxitjen e respektimit të të drejtave të njeriut në bazë të raporteve apo studimeve që i paraqiten si shteteve anëtare, ashtu edhe Asamblesë së Përgjithshme dhe Agjensive të

Specializuara.

- Autorizon Këshillin Ekonomik dhe Social të Kombeve të Bashkuara/ ECOSOC të ngrejë komisione në fushat ekonomike dhe sociale për nxitjen e të drejtave të njeriut, si dhe komisione të tjera të cilat nevojiten për përmbushjen e funksioneve të saj.

Vlen të përmendet se Karta e Kombeve të Bashkuara përmban vetëm referenca këshilluese për të drejtat dhe liritë e njeriut; për më tepër edhe neni 56 i saj, ku sanksionohet se të gjithë anëtarët "zotohen", është jo detyrues.

2.1.2 Deklarata Universale për të Drejtat e Njeriut/UDHR

Deklarata Universale për të Drejtat e Njeriut vlerësohet nga shumë teoricienë modernë që studiojnë jurisprudencën si dokumenti ndërkombëtar i vetëm dhe më i rëndësishëm që është shkruar ndonjëherë, ku ka kontribuar në nxitjen e të drejtave të njeriut si rezultat i një sërë arsyesh që kanë ndikuar në këtë pohim:

- Momenti kur u përpilua dhe konteksti historik global
- Influenca e jashtëzakonshme që ka patur në dokumentet dhe regjimet e të drejtave të njeriut që kanë pasuar në vazhdim
- Për shkak të faktit që edhe pse ky dokument është një deklaratë dhe jo traktat, ende ka shumë individë që besojnë se dokumenti gëzon statusin e të drejtës ndërkombëtare zakonore

Kjo deklaratë njohu veprat e dhunshme kriminale që ka dëshmuar historia duke lënduar thellë ndërgjegjen shoqërore të njerëzimit, si dhe njohu gjithashtu dinjitetin themelor dhe të drejtat e patjetërsueshme për të gjitha qëniet humane, që kanë nevojë të bazohen në liri, paqe dhe drejtësi.

Gjithashtu, kjo deklaratë shkoi më tej, duke e vënë theksin tek fakti se duke u konsideruar intrument ndërkombëtar do të përpiqej të vendoste një standart (të arritur ndërmjet shkollimit në këtë fushë) me qëllim që të rrisë zbatimin dhe të sigurojë njohjen universale të të drejtave të njeriut.

Edhe këtu është parashikuar shprehimisht mosndërhyrja arbitrare në jetën private, familjen, shtëpinë apo korrespondencën, sanksionuar konkretisht në Nenin 12 të kësaj deklarate.

2.1.3 Paktet Ndërkombëtare

Paktet Ndërkombëtare u krijuan duke patur si qëllim zëvendësimin e

Deklaratës në një formë të risjellë më evoluese meqënëse parashikonin dhe një dokument ligjor me karakter detyrues. Tashmë dispozitat e Deklaratës Universale për të Drejtat e Njeriut u konvertuan në dy instrumente ndërkombëtarë: Pakti Ndërkombëtar i të Drejtave Ekonomike, Sociale dhe Kulturore[5], si dhe Pakti Ndërkombëtar i të drejtave Civile dhe Politike [6].

2.2 Mekanizmat institucionalë të Kombeve të Bashkuara për mbrojtjen dhe promovimin e të drejtaës për respektimin e jetës private, si një ndër të drejtat themelore të njeriut

Sistemi i mbrojtjes dhe promovimit të të drejtave të njeriut të Kombeve të Bashkuara përmban dy lloj tipe strukturash:

- Strukturat e krijuara nga Karta e Kombeve të Bashkuara, përfshirë Komisionin e të Drejtave të Njeriut, si dhe
- Strukturat e krijuara nga traktatet ndërkombëtare të të drejtave të njeriut

Në fakt është struktura organizuese e Kombeve të Bashkuara për të drejtat e njeriut ajo që është direkt përgjegjëse për të drejtat e njeriut, si dhe për sigurimin e qëllimit të Kombeve të Bashkuara për të siguruar universalitetin e të drejtave të njeriut, duke nënkuptuar këtu njohjen e plotë të dinjitetit, barazisë dhe vlerës që mbart çdo qënie njerëzore.

Asambleja e Përgjithshme është institucioni ndërkombëtar që ndodhet në majë të hierarkisë midis organeve të Kombeve të Bashkuara. Megjithatë, Këshilli i Sigurimit mbart disa përgjegjësi për të drejtat e njeriut të cilat bëhen primare kur vihet në rrezik paqja dhe siguria ndërkombëtare. Ndërsa, Komisioni i të Drejtave të Njeriut nën drejtimin e Komisionerit të Lartë për të Drejtat e Njeriut, e ka zgjeruar tashmë rolin e tij, duke iu përgjigjur problematikave që cënojnë liritë e individit në një shkallë të plotë.

Gjithashtu, një rol të rëndësishëm dhe në rritje e sipër ka edhe Nënkomisioneri mbi Promovimin dhe Mbrojtjen e të Drejtave të Njeriut, Raportuesit Tematikë dhe Shtetërorë, si dhe grupet e punës të cilët raportojnë tek Komisioneri. Nuk duhet lënë pa u përmendur edhe roli mbrojtës që siguron Këshilli Ekonomik dhe Social, pasi ndërmjet tij kalojnë shumica e raporteve zyrtare që prej këtej shqyrtohen më pas nga Asambleja e Përgjithshme.

Përveç institucioneve të ngritura prej Kartës së Kombeve të Bashkuara ekzistojnë shtatë organe-Komitete, të krijuara nga traktatet kryesore të të drejtave të njeriut, të cilat monitorojnë zbatimin e çdo traktati. Disa prej

strukturave monitoruese të traktateve janë: Komiteti i të Drejtave të Njeriut; Komiteti mbi të Drejtat e Fëmijëve; Komiteti mbi të Drejtat Ekonomike, Sociale dhe Kulturore etj. Komitetet e lartpërmendura bashkëpunojnë ngushtësisht me Këshillin Ekonomik dhe Social, si dhe me Asamblenë e Përgjithshme për të siguruar përmbushjen me efikasitet të qëllimit për të cilat janë krijuar.

Gjykatat Ndërkombëtare

Brenda OKB –së veprojnë edhe dy gjykata ndërkombëtare për të siguruar drejtësi për çdo individ që i është cënuar e drejta e tij për të patur një jetë private dhe familjare të mbrojtur me ligj. Këto gjykata janë:

Për më shumë shih: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx

Për më shumë shih: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

- Gjykata Ndërkombëtare e Drejtësisë, e cila është krijuar nga Karta e Kombeve të Bashkuara dhe funksionon si gjykatë me shtrirje globale
- Gjykata Ndërkombëtare Penale, e cila u krijua me një statut të pavarur në vitin 2002

3. Mbrojtja ligjore që ofron Bashkimi Europian për mbrojtjen e privatësisë nga zhvillimet teknologjike

Për arsye që lidhen me shtrirjen ndërkombëtare që kanë marrë veprat penale për shkak të zhvillimit teknologjik, si dhe për arsyen e shfaqjes së formave të reja të integruara të kriminalitetit, ka një vëmendje të shtuar të organizmave ndërkombëtarë me qëllim pengimin e shtrirjes më tej dhe luftimin e këtyre formave të reja të veprave penale. Për tia arritur këtij qëllimi Këshilli i Europës ka miratuar disa rekomandime.

Rëndësi ka edhe miratimi i Rezolutës nr.1 nga Ministrat Europianë të Drejtësisë prezantuar gjatë konferencës së tyre, mbajtur në Pragë më 1997, e cila i rekomandonte Komitetit të Ministrave të mbështeste aktivitetet në lidhje me kiberkriminalitetin që organizohet nga Komiteti Europian për problemet me natyrë kriminale. Qëllimi është të përafrohen legjislacionet penale kombëtare dhe të bëhet e mundur përdorimi i mjeteve efikase të hetimit në fushën e veprave kriminale teknologjike që cënojnë privatësinë e

individit.

Me këtë frymë, më 23 Nëntor të 2001 u nënshkrua në Budapest "Konventa mbi Kiberkriminalitetin". Ky instrument është plotësuar nga një protokoll shtesë në lidhje me inkriminimin e akteve që cënojnë dinjitetin e njeriut duke përdorur sistemet informatike, i nënshkruar në Strasburg më 28 Janar 2003.

Me qëllim krijimin e një rregulloreje për parandalimin dhe luftimin e veprave penale teknologjike që cënojnë privatësinë e personit, shtetet anëtare të Këshillit të Europës dhe shtete e tjera nënshkruese duke konsideruar që qëllimi i Këshillit të Europës është që të arrihet një unitet sa më i madh ndërmjet anëtarëve të tij në nxitjen e bashkëpunimit midis shteteve ndërmjet nënshkrimit të Konventës së Budapestit, bën të mundur ndjekjen në mënyrë prioritare për një politikë penale të përbashkët, që ka si qëllim mbrojtjen e shoqërisë nga krimi kibernetik që cënon jetën private të personit, midis të tjerash adaptimin e nje legjislacioni të përshtatshëm dhe nxitjen e bashkëpunimit ndërkombëtar ku shoqëritë dhe mekanizmat e tyre ligjore të ndërgjegjësohen e të përgatiten për risitë që sjell konvergjenca, dixhitalizimi dhe globalizimi i vazhdueshëm i rrjeteve kompjuterike.

3.1 Direktiva 95/46 – KE "Për mbrojtjen e të Dhënave Personale"

Direktiva 95/46 – KE është teksti kryesor i referimit në nivel europian për sa i përket tematikës së mbrojtjes së të dhënave personale. Kjo direktivë mbulon cilëndo formë të përpunimit të të dhënave personale pa marrë në konsideratë teknologjinë e përdorur. Qëllimi kryesor i direktivës është të mbrojë të drejtat dhe liritë themelore të individit dhe në mënyrë të veçtë të drejtën për jetë private lidhur me proceset përpunuese të të dhënave personale duke parashtruar standartet bazë që duhet të respektohen nga ana e subjekteve përpunuese.

3.2 Direktiva 2002/58 – KE për "e-Privatësinë"

Direktiva 2002/58 sqaron dhe plotëson më tej Direktiva 95/46 për sa i përket përpunimit të të dhënave personale në sektorin e komunikimeve elektronike dhe njihet gjerësisht si Direktiva e Privatësisë. Direktiva synon në mënyrë të veçantë të sigurojë respektimin e plotë të të drejtës për jetë private dhe gjithashtu, të drejtës për mbrojtjen e të dhënave personale të parashikuar në nenet 7 dhe 8 të Kartës së të Drejtave Themelore të Bashkimit Europian.

3.3 Direktiva 2006/24 – KE "Mbi Ruajtjen e të Dhënave"

Direktiva 2006/24 ka si qëllim të harmonizojë kuadrin ligjor të shteteve anëtare të Bashkimit Europian për sa i takon detyrimeve të sipërmarrësve të shërbimeve dhe të rrjeteve të komunikimeve publike elektronike për ruajtjen e të dhënave të caktuara që përpunohen dhe administrohen prej tyre, në mënyrë që këto të dhëna të vihen në dispozicion të autoriteteve të ndjekjes penale me qëllim zbulimin, hetimin dhe ndjekjen e veprave penale, ashtu sikundër përcaktohet në legjislacionet kombëtare të gjithësecilit shtet.

4. Mbrojtja juridike që i bën legjislatori ynë i brendshëm respektimit të privatësisë:

Që në hyrje të Kushtetutës, e më konkretisht në Nenin 3 të saj, ndër të tjera vlera të përmendura, legjislatori ynë ka parashikuar shprehimisht se dinjiteti i njeriut dhe të drejtat dhe liritë e tij janë bazat ku shteti ka detyrimin ligjor ti mbrojë.

I vihet theksi më tej kësaj mbrojtjeje në Nenin 15 të Kushtetutës ku është i sanksionuar pohimi se *"1. Të drejtat dhe liritë themelore të njeriut janë të pandashme, të patjetërsueshme e të padhunueshme dhe qëndrojnë në themel të të gjithë rendit juridik.*

2. Organet e pushtetit publik, në përmbushje të detyrave të tyre, duhet të respektojnë të drejtat dhe liritë themelore të njeriut, si dhe të kontribuojnë në realizimin e tyre. "

Vijohet më tej garancia proceduriale me Nenin 35 të Kushtetutës[7] ku flitet konkretisht për të dhënat personale, ku ndalohet shprehimisht cënimi i jetës/i të dhënave private.

5. Pasojat që ndihen në praktikë si rezultat i cënimit të së drejtës për të patur një jetë private

Për të drejtën natyrore universale që duhet të gëzojë çdo individ për t'iu respektuar jeta private dhe familjare, është praktika ajo që gjithmonë ka dëshmuar se kjo e drejtë e qënësishme e njeriut lehtësisht në ditët e sotme mund të cënohet nga zhvillimet e pajisjeve teknologjike, të cilat do ti identifikojmë si më poshtë vijon:

Neni 35 i Kushtetutës së Republikës së Shqipërisë sanksionon se:

"*1. Askush nuk mund të detyrohet, përveçse kur e kërkon ligji, të bëjë publike të dhëna që lidhen me personin e tij.*

2. Mbledhja, përdorimi dhe bërja publike e të dhënave rreth personit bëhet me pëlqimin e tij, me përjashtim të rasteve të parashikuara me ligj.

3. Kushdo ka të drejtë të njihet me të dhënat e mbledhura rreth tij, me përjashtim të rasteve të parashikuara me ligj.

4. Kushdo ka të drejtë të kërkojë ndreqjen ose fshirjen e të dhënave të pavërteta ose të paplota ose të mbledhura në kundërshtim me ligjin."

- Mjetet mediatike

Në çështjen që do trajtohet në paragrafët e mëposhtëm të këtij punimi "William Sidis vs New York Post"[8] kuptohet më qartazi se si ndikimi i medias i kalon kufijtë e të qënurit thjesht burim informacioni, pasi ajo duke përdorur zhvillimin e pajisjeve teknologjike, siç është media e shkruar në rastin konkret, humbet funksionin për të cilin është krijuar dhe kthehet në burim të pavërtetash duke cënuar fillimisht privatësinë e individit që targëzon, e ku rrjedhimisht prej këtej kalohet më pas në cënimin e integritetit dhe dinjitetit të personit, duke shkelur/dhunuar në këtë mënyrë haptazi, të drejtën natyrore universale të individit për të patur një jetë private.

William James Sidis konsiderohet si gjeniu i matematikës. Ai lindi në vitin 1898 në Manhatan të qytetit njujorkez, ku prindërit e tij ishin emigrantë hebrenj që u kishin shpëtuar masakrave kundër komunitetit të tyre në Ukrainë në vitet 1880. Me një koeficient inteligjence (IQ) prej 250-300, ai u përshkrua si "djali gjeni" nga gazeta "The Washington Post". Në moshën 9 vjeçare ai dha provimin e hyrjes në Universitetin e Harvardit, ndërsa kur mbushi 11 vjeç ligjëroi për herë të parë në Klubin e Matematikanëve të Harvardit. U diplomua me nota maksimale 5 vjet më vonë. Por Uilliam nuk arriti që të ketë ndonjë sukses të madh të mëtejshëm, pavarësisht intelektit të tij të jashtëzakonshëm, kjo në sajë të ndërhyrjes që media pati duke cënuar integritetin e tij.

Ndërkohë që Uilliami nisi të shfaqej në kopertinat e revistave të njohura, ai vuante,pasi e nuk donte vëmendjen. Atij i pëlqenin rregullat dhe rutina, duke dëshiruar një jetë të qetë private larg vëmendjes mediatike. Ai nisi punë si pedagog i matematikës në Institutin Rajs në Hjuston të Tekasit, por duke qenë shumë më i ri studentët nuk e merrnin seriozisht dhe pas kësaj përvoje Uilliam e shmangu jetën publike, duke kaluar nga një punë e rëndomtë në tjetrën.

Por shtypi e zbuloi rutinën e tij dhe më 1937, gazeta prestigjoze "The New York Post" – gazeta më e madhe e kohës që konsiderohej si e tillë edhe për Europën, i dedikoi një artikull me titull "Gjeniu fëmije i vitit 1909, tani paguhet si nëpunës i rëndomtë për 23 dollarë në javë". Aty e portretizonin Uilliamin si një dështim që nuk e kishte përmbushur premtimin e tij të fëmijërisë së hershme, për karrierë të mëtejshme që do i sillte lavdi SHBA-ve. I gjendur përballë presionit mediatik, Uilliam vendosi të dilte sërish në qendër të vëmendjes, por kësaj here duke e paditur gazetën e "New York Post" për shpifje, në atë që sot konsiderohet si *padia e parë për shkeljen e privatësisë*.

Historia e Uilliam Sidis shërben për të ngritur edhe në ditët e sotme disa pyetje që jurisprudenca është ajo e cila ndërhyn për të dhënë përgjigjen e drejtë: A duhet t'i nënshtrohen të miturit një presioni kaq të madh në një moshë kaq të hershme? Dhe si përfundim, a kanë të drejtë personat publikë të kenë një jetë private?!

- Mjetet elektronike të komunikimit publik
- Vjedhja e identitetit dhe impersonifikimi online

https://pamfleti.net/william-sidis-historia-tragjike-e-njeriut-me-te-zgjuar-ne-bote/

Vjedhja e identitetit përkufizohet si mbajtja, transferimi i paligjshëm, ose keqpërdorimi i informacionit personal me qëllim kryerjen e një krimi tjetër. Autorët e konsumojnë këtë vepër penale të dytë duke u nxitur nga dy qëllime të ndryshme: Ose për të kanosur personin që i vjedh identitetin (i motivuar nga arsye personale), ose për të nxjerrë përfitime monetare nga persona të tretë duke shfrytëzuar identitetin e vjedhur të viktimës.

Ndërsa mënyrat dhe format e përdorura nga autorët e krimeve teknologjike për të kryer vjedhjen e identitetit të një personi në rrjete sociale janë si më poshtë:

- Së pari, duke vjedhur të dhënat identifikuese të llogarisë së viktimës në rrjetin social, dhe
- Së dyti, duke krijuar një profil të ri me të dhëna tërësisht të rreme dhe duke u shtirur si një person tjetër

Rasti më i fundit që ka si temë vjedhjen e identitetit dhe të impersonifikimit online ka ndodhur në vendin tonë ka vetëm disa ditë më parë. Autori 39-vjeçar me iniciale E. M., banues në Tiranë, u arrestua pasi hapte llogari false në rrjete sociale duke përdorur të dhënat dhe fotot e shtetasve të tjerë. Operacioni policor është finalizuar pas denoncimit që një vajzë ka bërë, pasi autori

kishte hapur vazhdimisht llogari në rrjetet sociale me të dhënat dhe fotot e saj personale. Pas verifikimeve të kryera nga specialistët e krimit kibernetik ka rezultuar se ky shtetas ka hapur në mënyrë të vazhdueshme llogari. Materialet procedurale i kaluan Prokurorisë për veprime të mëtejshme, ku më pas do të gjykohet për veprën penale "Falsifikimi kompjuterik". Por, siç bëjnë me dije autoritetet, autori i këtij krimi nuk është një emër i panjohur për drejtësinë, pasi ka qenë më parë i arrestuar edhe për vjedhje me dhunë.(9)

Shembuj të shfrytëzimit të identiteteve të rreme duke përdorur rëndom rrjetet sociale të tilla si: Facebook, Instagram apo What's up, praktika jonë dhe ajo ndërkombëtare njohin pafund, por ajo çfarë e bën më shqetësuese fenomenin është se praktika ligjore e çdo shteti po tregon se me rritjen e sofistikimit të mjeteve elektronike, aq më tepër po vihet re një tendencë në rritjeje e veprave penale që po kanosin jetën private të individit duke përdorur mjetet e teknologjisë së avancuar për tia arritur qëllimit të tyre kriminal.

❍ Inteligjenca Artificiale

Teknologjia e njohjes së fytyrës, është kritikuar shpesh për shkelje të privatësisë së individëve. Por në një kompani në Kinë, kjo teknologji shkon më tej. "Canon China", një degë e gjigantit japonez të kamerave dhe elektronikës, do vetëm punëtorë të lumtur. Për këtë arsye, kompania ka aplikuar teknologjinë e njohjes së buzëqeshjes. (10)

https://top-channel.tv/2022/06/14/hapte-llogari-false-ne-rrjete-sociale-me-te-dhena-dhe-fotot-e-shtetasve-te-tjere-arrestohet-39-vjecari-ne-tirane/ https://www.botasot.info/life-style-showbiz/1645152/duam-vetem-punetore-te-lumtur/

Kamera të pajisura me inteligjencë artificiale janë vendosur në hyrje të ndërtesës. Hyrja u lejohet vetëm punonjësve që arrijnë t'i bindin me buzëqeshje se janë të lumtur. Në Canon, "detyrimin" për të buzëqeshur e justifojnë duke pohuar se këtë metodë e përdorin me qëllim krijimin e atmosferës pozitive në punë.

Monitorimi i punonjësve duke përdorur pajisje me inteligjencë artificiale është kthyer në praktikë të zakonshme për disa kompani të mëdha. "Amazon", bën pjesë tek ato kompani që gjurmon stafin dhe përdor inteligjencën artificiale për të vlerësuar performancën e tyre. Mbi informacionin e mbledhur bëhen ngritjet në detyrë dhe shkarkimet. Gjithnjë e më shumë punëdhënës po përdorin softuer të monitorimit në distancë për të mbajtur nën kontroll punonjësit nga shtëpia.

Sipas një studimi të "Smarter With Gartner", më shumë se gjysma e bizneseve të mëdha të anketuara po përdorin një lloj mbikëqyrjeje, nga analizimi i postave elektronike e deri tek mbledhja e të dhënave biometrike. Disa po përdorin kamera në internet për të monitoruar vëmendjen e punonjësve. Ata mund të vlerësojnë nëse punonjësit kanë vëmendjen e duhur thjesht ndjekur lëvizjet e tyre të syve dhe gjuhën e trupit.

6. KONKLUZIONE dhe REKOMANDIME

Paketa e parë ligjore europiane që trajton ligjet me karakter teknologjik, e kryesisht ligjet mbi krimet kompjuterike është "Konventa e Këshillit të Europës mbi Krimet Kibernetike" shpallur në vitin 2001, ndërkohë që paketa e dytë e miratuar nga Bashkimi Europian përmban vetëm funksion rregullator në lidhje me veprat penale të shkaktuara nga ndërhyrjet teknologjike të kompjuterit, duke siguruar në këtë mënyrë mbrojtje të plotë ligjore për viktimat që iu cënohet respektimi i jetës private nga ndërhyrjet e pakontrolluara teknologjike.

Ndërsa konkretisht vendi ynë për të parandaluar dhe luftuar krimin kibernetik ka ratifikuar "Konventën e Budapestit mbi Krimin Kibernetik", si dhe ka përfshirë disa vepra penale në Kodin Penal ndërmjet ligjit Nr.10023, datë 27.11.2008 të ndryshuar [11], në kuadër të përafrimit dhe harmonizimit të legjislacionit tonë të brendshëm në përputhje me parashikimet e Konventës së lartpërmendur.

Ligji Nr.7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar, tregron haptazi për një përmirësim dhe përafrim të legjislacionit tonë me acquis – in e BE – së, pasi ndër të tjera ndryshime efektive, është sanksionuar edhe kjo shtesë në përmbajtjen e nenit 7:

Neni 1

Në fund të nenit 7 shtohet shkronja "j" me këtë përmbajtje:

"j) vepra penale në fushën e teknologjisë së informacionit.".

Gjithashtu, do të konsiderohet pozitive fakti që pas nenit 293/c është shtuar neni 293/ç, i cili parashikon si vepër penale keqpërdorimin e pajisjeve teknologjike, sipas të cilit prodhimi, mbajtja, dhënia në përdorim, shitja, shpërndarja apo çdo veprim tjetër për vënien në dispozicion të një pajisjeje,

ku përfshihen edhe program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim krryerjen e veprave penale të parashikuara në nenet: 192/b, 293/a, 293/b dhe 293/c.

Si një ndër masat rekomanduese tejet produktive do të ishte përsosja dhe plotësimi më tej i kuadrit ligjor në fushën e sigurisë kibernetike, ku për të arritur deri në harmonizimin ideal të legjislacionit tonë të brendshëm sugjerohet se duhet të bëhet vlerësimi i praktikave më të mira botërore dhe të merren në konsideratë rekomandimet e raporteve ndërkombëtare.

Përsëri në kuadër të përafrimit të legjislacionit tonë të brendshëm vlerësohet se duhet ti kushtohet rëndësi përfshirjes së një dispozite të re në Kodin Penal ku të trajtohen më gjerësisht dhe specifikisht ato çështje që kanë të bëjnë me impersonifikimin online. Sugjerojmë që si dispozitë e re të mund të vendoset krahas neneve 121 – 123 të Kodit Penal që mbrojnë të drejtat e individit për jetë private.

Gjithashtu, në kuadër të mbrojtes së viktimave nga mjetet teknologjike, duhet të merret në konsideratë shtimi i investimeve për të realizuar rritjen e sigurisë në rrjetet dhe sistemet shtetërore, për të bërë të mundur shmangien e rrjedhjes së informacionit të aspekteve identifikuese të personave duke cënuar në këtë mënyrë jetën private të tyre. Duke u ndalur këtu, duhet ti jepet prioritet prioritet shtimit të investimeve në hardëare dhe softëare, për të siguruar parandalimin në raste të përballjes me vepra penale të atilla, ashtu sikurse ka treguar praktika jonë.

Si rekomandim tjetër do të ishte krijimi i një Autoriteti Kombëtar i Zhvillimit Teknologjik, ku fare mirë mund të funksionojë si ministri shteti, duke patur në përbërje të tij specialistë të fushave të ndryshme të IT – së, si dhe juristë të specializuar në hetimet dhe gjurmimin e krimeve kibernetike. Vlerësohet se duke qënë një institucion në nivel ministror do jetë më monopolizues dhe do të kursente kohë e kosto për çështjet që do të merrte në trajtim duke ofruar jo vetëm mbrojtje gjithëpërfshirëve për viktimat që iu kanoset jeta private nga mjetet teknologjike, por gjithashtu do të bënte të mundur shmangien për të ndodhur të fenomeneve të tilla globale.

I një rëndësie të veçantë është edhe bashkëpunimi, koordinimi dhe harmonizimi institucional, tashmë jo vetëm brenda institucioneve kompetente me njëra tjetrën për trajtimin e veprave penale që cënojnë jetën private të individit duke përdorur mjetet e sofistikuara teknologjike, por kjo shtrirje bashkëpunimi duhet të bëhet gjithmonë e më prezente me institucionet

dhe mekanizmat ndërkombëtarë me përvojë të gjerë në këtë fushë, siç janë Europoli dhe Eurojusti.

Gjithashtu, kjo përvojë institucionale duhet të ndahet edhe me universitetet - ashtu sikurse edhe vetë akademitë e universitetet në koordinim me njëri tjetrin, ku një rëndësi marrin organizimi i trajnimeve, workshopeve, seminareve dhe konferencave për të evidentuar praktikat më efikase në parandalimin e veprave penale të tilla dhe mbrojtjen e individit nga këto dukuri teknologjike.

Por, si një masë adekute, të cilën edhe praktikat botërore e kanë vlerësuar si masën më efektive për mbrojtjen e jetës private, sugjerohet të jetë edukimi dhe rritja e ndërgjegjësimit për krimet teknologjike në mesin e individëve. Kjo realizohet duke ndërmarrë fushata informuese për popullatën, në bashkëpunim me median, institucionet dhe ojf - të që operojnë në Shqipëri. Ky informim bëhet me mënyra e forma të ndryshme, si ndërmarrja e fushatave dhe reklamave/spoteve informuese dhe atyre ndërgjegjësuese, trajtimi nëpër emisione i tematikave të tilla, duke përfshirë edhe MASR – në etj.

Në përfundim të këtij materiali ia vlen të përmendim citatin e shprehur nga A. Einstein, për të sjellë edhe njëherë në vëmendje faktin e pamohueshëm se burimet teknologjike, ashtu sikurse na e kanë lehtësuar përditshmërinë me sofistikimin e tyre, me kalimin e kohës dhe supersofistikimin që ato po marrin, janë dalëngadalë "duke na marrë" edhe jetën private; ndaj ne – qëniet humane duhet të bëjmë gjithçka kemi mundësi, sa jemi koshientë dhe në kohë, përpara se të jetë vonë për të kuptuar se po na cënohet një e drejtë njerëzore që në thelb nuk është gjë tjetër veçse natyrore dhe universale!

"*Kam frikë nga dita kur teknologjia të kalojë kapacitetin intelektual të njeriut. Bota do të ketë një brez idiotash.*"

(Albert Einstein)

REFERENCAT:

- Kushtetuta e Republikës së Shqipërisë
- Kodi Penal i Republikës së Shqipërisë, i ndryshuar
- Konventa Europiane e të Drejtave të Njeriut
- Konventa e Budapestit "Mbi Krimet Kibernetike"
- Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly,

Identifying, Understanding and Analyzing Critical Infractructure Interdependencies, IEEE Control Systems Magazine, December 2001

- Calvo, C. (1885), *Le Droit International*, 5th ed Paris, (përkthyer nga origjinali në gjuhën spanjolle, *Derecho international teorico and practico*, 1868, Paris)
- Root, E., (1930), *The basis of protection of citizens residing abroad, American Journal of International Law*, No.24
- Muçollari, O., *Të drejtat ndërkombëtare të njeriut*, cikël leksionesh, Tiranë 2014
- Direktiva 95/46 e KE - së "Për mbrojtjen e të Dhënave Personale"
- Direktiva 2002/58 e KE - së për "e-Privatësinë"
- Direktiva 2006/24 e KE - së "Mbi Ruajtjen e të Dhënave"
- https://pamfleti.net/william-sidis-historia-tragjike-e-njeriut-me-te-zgjuar-ne-bote/
- https://top-channel.tv/2022/06/14/hapte-llogari-false-ne-rrjete-sociale-me-te-dhena-dhe-fotot-e-shtetasve-te-tjere-arrestohet-39-vjecari-ne-tirane/
- https://www.botasot.info/life-style-showbiz/1645152/duam-vetem-punetore-te-lumtur/

ALTERNATIVAT E KRIMIT TË ORGANIZUAR NË SHQIPËRI, DHE NDIKIMI I KRIMIT KIBERNETIK.

DR. GENADA TAHO

Fakulteti i Shkencave Politike-Juridike / Universiteti "Aleksandër Moisiu" Durrës

genada.taho@fdut.edu.al

DR. IVAS KONINI

Fakulteti i Drejtësisë / Universiteti i Tiranës

Ivas.konini@fdut.edu.al

Abstract

Krimi i organizuar në Shqipëri po shfaqet gjithmonë e mëindërlikuar dhe dinamik. Ai shfaqet si kërcënues i demokracisë, shtetit të së drejtës dhe të drejtave të njeriut, stabilitetit si dhe progresin e një vendi. Natyra komplekse dhe në ndryshim të vazhdueshëm shton kërcënime të reja për një shoqëri në tranzicion si e jona dhe impakti i tij shtrihet edhe përtej vendit.

Nën ndikimin e fuqishëm të faktorëve të ndryshëm lokal, rajonal dhe global, janë zhvilluar dhe përsosur format e krimit të organizuar si trafikimi i narkotikëve, i qënieve njerëzore, i armëve, krimet kibernetike dhe pastrimi i parave. Ndër faktorët më të rëndësishëm që nxisin dhe zhvillojnë krimin e organizuar, përmendim faktorë me karakter ekonomikë, politikë dhe social.

Krimi kibernetik është një ndër krimet që me përsosjen e teknologjisë, priret gjithmone e më shumë drejt rritjes dhe sofistikimit, element ky që

sjell vështirësinë e goditjes së tij.Edhe format e tjera të krimit të oganizuar gjithmonë e më shumë po përdorin teknologjinë për arritjen e synimeve të tyre kriminale.

Arsyet e dështimit të agjensive ligjzbatuese në goditjen e këtij fenomeni në nivel kombëtar dhe ndërkombëtar,lidhen me bashkëpunimin e dobët, shkëmbimin e infomacionit në shkallë të gjerë dhe mungesën e koordinimit midis agjensive të ndryshme ligjzbatuese, si dhe konsolidimin e punonjësve të specializuar në këto institucione.

Besimi te drejtësia vazdon të jetëi ulët dhe shoqëria shqiptare shfaqet nguruese në denoncimin e këtyre fenomeneve.

Fjakë kyce: krim i organizuar, krim kibernrtik, trafikim, pastrim parash

1. Koncepti i krimit të organizuar.

Në literaturën e së drejtës penale shqiptare, krimi i organizuar është konsideruar si shkalla më e lartë e organizimit të kriminalitetit profesionist dhe me krim të organizuar nënkuptohet krijimi i grupeve dhe bandave të ndryshme të organizuara që bashkëpunojnë në mënyre të rregullt për kryerjen e veprave penale.[1] Por çfarë kuptohet me nocionin e krimit të organizuar në të drejtën penale shqiptare? Ashtu si fenomeni, edhe nocioni i krimit të organizuar në të drejtën penale shqiptare është i vonshëm dhe nuk ka një përkufizim të mirëfilltë e të gjithëpranuar për të, megjithëse përdoret shpesh nga literatura dhe praktika si nocion.

Në Shqipëri termi krim i organizuar është një term të cilin nuk e gjejmë as në Kodin Penal. Në të parashikohen vetëm format e bashkëpunimit të veçantë[2], por pa i cilësuar këto të fundit në mënyrë eksplicite si krim i organizuar. Termi krim i organizuar nuk ndeshet as në ligjet penale materiale që parashikojnë vepra penale. Edhe në ligjin kundër krimit të organizuar,[3]nuk ekziston një përkufizim formal ligjor për të. Për këtë arsye, kuptimi i krimit të organizuar, mund të trajtohet vetëm në planin doktrinal, në të cilin nuk ka një përkufizim të vetëm teorik për të.

Doktrina e klasifikon krimin e organizuar si formë të veçantë bashkëpunimi, duke iu referuar ndryshe edhe si shkalla më e lartë e

1 Elezi I, "Vështrim mbi zhvillimet e legjislacionit penal shqiptar kundër krimit të organizuar" në "Gjendja e krimit të organizuar në Shqipëri, Kosovë, Mal të Zi, Maqedoni si dhe problemet që lidhen me të" Tiranë, Dhjetor 2002. fq. 9

2 Neni 28, Kodi Penal I RSH. Tirane 1995, i përditësuar

3 Ligji nr. 9284 datë 30.09.2004 "Për parandakimin dhe goditjen e krimit të organizuar"

bashkëpunimit me rrezikshmërinë shoqërore më të madhe, dhe me të cilin do të kuptojmë krijimin e grupeve dhe bandave të ndryshme të organizuara që bashkëpunojnë në mënyrë të rregullt për kryerjen e veprave penale.[4]

Pavarësisht mungesës së një përkufizimi përfundimtar e unik mbi krimin e organizuar nga legjislacioni penal shqiptar, përcaktimi i këtij nocioni bëhet nga Konventa e Kombeve të Bashkuara "Kundër Krimit të Organizuar Ndërkombëtar"[5], dhe si rrjedhojë është e detyrueshme për zbatim nga organet ligjzbatuese shqiptare. Konventa në nenin 2/a të saj jep konkretisht përkufizmin e grupit kriminal të organizuar: grup kriminal i organizuar nënkupton një grup të strukturuar, i cili ka ekzistuar për një periudhë kohe të caktuar, i përbërë nga tre ose më shumë persona, të cilët veprojnë në harmoni me njëri-tjetrin, me qëllim që të kryejnë një ose më shumë krime ose vepra penale serioze, të përcaktuara si të tilla në përputhje me dispozitat e kësaj Konvente, me qëllim që të sigurojnë, në mënyrë direkte ose indirekte, perftime financiare ose materiale.

Nisur nga ky përkufizim mund të nxjerrim kriteret të cilat duhet të plotësohen në mënyrë që një vepër penale të konsiderohet krim i organizuar:

1. Kërkohet bashkëpunimi i tre ose më shumë personave;
2. Nga pikëpmja kohore stukturat e krimit të organizuar duhet të kenë ekzistuar për një periudhë kohe të caktuar, pra për një periudhë të zgjatur;
3. Kryeja krimeve me rrezikshmëri shoqërore të lartë ose veprave penale serioze sipas përcaktimeve të Konventës;
4. Qëllimi i përfitimeve materiale dhe/ose jomateriale.

Pra sipas përkufizimit të Konventës, duhet të ekzistojnë kriteret e sipërpërmendura në mënyrë që një vepër penale të kosiderohet krim i organizuar, kritere të cilat kanë shërbyer për përkufizimin e të gjitha formave të veçanta të bashkëpunimit nga Kodi Penal aktual. Ky i fundit në nenin 28 të tij parashikon si forma të veçanta të bashkëpunimit në kryejen e veprës penale organizatën kriminale, organizatën terroriste (si formë e të parës), bandën e armatosur dhe grupin e strukturuar kriminal, duke përcaktuar disa elementët përbërës të secilës formë por dhe për të bërë dallimet nga një formë tek tjera.[6]

---

4 Zhilla.F, Lamallari. B, Raport "Vleresimi i riskut të krimit të organizuar në Shqipëri", Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015, fq 17

5 Ligj nr. 8920, datë 11.7.2002 Për ratifikimin e "Konventës së Kombeve të Bashkuara kundër krimit të organizuar ndërkombëtar" dhe dy protokolleve shtesë të saj

6 Hoxha.D, Kaçupi.S, Haxhia.M "E Drejta Penale, Pjesa e Përgjithshme", Botimet Jozef, Durrës 2018, fq 482

2. Faktorët e zhvillimit të krimit të organizuar.

Raporte të ndryshme kombëtare dhe ndërkombëtare të agjencive ligjzbatuese dhe organizatave të pavarura e kanë pranuar prej kohësh ekzistencën e krimit të organizuar në Shqipëri. Shfaqja dhe zhvillimi i krimit të organizuar në vend është nxitur dhe favorizuar nga faktorë të karakterit shoqëror, politik dhe ekonomik. Nga ana tjetër, shkalla e përhapjes dhe zhvillimit të këtij lloj kriminaliteti është përcaktuar nga niveli i reagimit institucional dhe shoqëror ndaj tij.

Kështu, fillesat e krimit të organizuar ne Shqipëri janë shënuar në periudhen e ndryshimit të sistemit totalitar në atë pluralist. Tranzicioni nga një sistem kontrolli total nga shteti, me një politikë të ashpër penale, drejt një sistemi të brishtë demokratik, u shoqërua me institucione të dobëta dhe me nëpunës pa edukimin dhe përvojën e mjaftueshme. Situata e krijuar në vitet 1997 dhe pasojat sociale dhe financiare të shkaktuara nga shembja e skemave piramidale kanë qenë një tjetër moment kyç në krijimin e kushte të favorshme për zhvillimin e krimit të organizuar në vend. Nga ana tjetër, dobësia e organeve të drejtësisë dhe policisë të mbërthyera nga korrupsioni dhe ndërhyrja apo kontrolli politik, ka lejuar pandëshkueshmërinë e eksponentëve të botës së krimit të organizuar.[7]

Në ndërthurje me mungesën e stabilitetit politik për mëse dy dekada në vend, kjo situatë ka krijuar hapësirat dhe mundësitë praktike të ndërveprimit, paraqitjes dhe përfshirjes në politikë të krimit të organizuar. Gjithashtu, kriza ekonomike e shoqëruar me nivele të larta papunësie dhe shkallë të lartë informaliteti ka favorizuar mundësitë e rekrutimit nga organizimet kriminale dhe investimit të tyre në ekonominë e ligjshme. Shpërbërja e strukturave tradicionale sociale, si familja dhe komuniteti ka lehtësuar përfshirjen e drejtpërdrejtë apo të tërthortë në veprimtari të organizuara kriminale fitimprurëse.

Një tjetër faktor i rëndësishëm që e ka bërë Shqipërinë një vend tërheqës për krimin e organizuar është pozita gjeografike midis vendeve prodhuese të drogës së fortë në Lindje, siç janë Afganistani dhe Turqia, dhe vendeve konsumatore në Perëndim, siç janë shtetet anëtare të BE-së. Gjithashtu konfliktet në rajon janë përmendur si faktor që ka shërbyer për hapjen e "rrugëve të trafikimit" dhe përfshirjen e krimit të organizuar shqiptar në rrjetet ndërkombëtare.

Valët e para dhe të vazhdueshme të migrimit, si dhe importimi i përvojes

7 Zhilla.F, Lamallari. B, Raport "Vleresimi i riskut të krimit të organizuar në Shqipëri", Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015, fq 18

dhe lidhjeve kriminale të fituara jashtë janë vlerësuar si faktorë përcaktues në sofistikimin e krimit të organizuar. Në këtë aspekt, pjesëtarë të diasporës shqiptare në vendet e BE-së, të cilët kanë hasur vështirësi në integrimin social dhe kulturor në vendin pritës, janë konsideruar një kontingjent me kosto minimale për zhvillimin e krimit të organizuar brenda dhe jashtë vendit. Përdorimi i gjerë i teknologjisë dhe mjeteve të zhvilluara të komunikimit ka lehtësuar dhe ndihmuar modernizimin e krimit të organizuar. Për më tepër, krimi i organizuar ka marrë përmasa ndërkombëtare si pasojë e globalizimit dhe, si çdo vend tjetër i prekur, Shqipëria nuk ka qenë një përjashtim.

Lidhur me rezultatet e agjencive ligjzbatuese shqiptare për parandalimin dhe luftën kundër krimit të organizuar, si dhe arsyet që mund ta kenë zbehur efikasitetin e punës së tyre, ekspertët kanë renditur si më kryesore nivelin e ulët të bashkëpunimit dhe bashkërendimit të punës midis agjencive të ndryshme, mungesën e konsolidimit të institucioneve që vazhdimisht iu nënshtrohen reformave në staf të kualifikuar sa herë ndryshojnë qeveritë, çështje të aspektit profesional, por dhe trajtimit të dobët financiar si në drejtim të pagave, infrastrukturës dhe logjistikës në dispozicion. Korrupsioni i zyrtarëve të caktuar, mosndëshkimi i tyre dhe mungesa e vullnetit për të përmbushur përgjegjësitë konkrete, janë përmendur nga shumica e të intervistuarve si një problem vërtet shqetësues.[8]

Faktorët kryesorë që studiuesit renditin për zhvillimin e kësaj forme të ashpër të kriminalitetit janë[9]:

- Vendosja e kontakteve midis elementeve me tendencë kriminale shqiptare me atë të vendeve fqinjë, marrja e eksperiencës së tyre si dhe formave të zhvillimit të këtij krimi.
- Ndërgjegjësimi i pakët i komunitetit për rrezikshmërinë dhe pasojat e krimit të organizuar.
- Fitimi maksimal i siguruar nëpërmjet krimit të organizuar për një periudhë kohe shumë të shkurtër.
- Niveli i lartë i varfërisë në të gjithë vendin.
- Pozicioni gjeografik i vendit në udhëkryqet midis lindjes dhe perëndimit.
- Niveli i ulët i reagimit të institucioneve të shtetit, për të përballuar,

8 Zhilla.F, Lamallari. B, Raport "Vleresimi i riskut të krimit të organizuar në Shqipëri", Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015, fq 8

9 Strategjia ndërsektoriale e luftës kundër krimit të organizuar, trafiqeve dhe terrorizmit, VKM 179, Gusht 2008, fq 6

goditur e ndërprerë lindjen dhe zhvillimin e formave të krimit të organizuar në Shqipëri.

- Mungesa e instrumentave ligjorë të nevojshëm në luftën kundër krimit të organizuar
- Rritja e korrupsionit sidomos në strukturat e zbatimit të ligjit, gjykatë prokurori, polici.

Për vite të tera, reagimi ndaj një situate kriminale në rriitje ka qënë i dobët, përforcuar dhe nga faktorë të tjerë si presioni, korrupsioni, frika, pasiguria, etj. Ishte presioni i madh nga organizmat ndërkombëtare dhe nga vete komuniteti që beri të ndërmerren hapa institucionale në luften kundër krimit të organizuar në Shqipëri si dhe disa formave të shfaqjes së tij, si luftës kundër trafikut të qënieve njerëzore të femrave apo fëmijëve. Luftës kundër trafikut të armëve, trafikut të lëndëve narkotike e kundër kultivimit të bimëve narkotike.

3. Krimi kibernetik, dhe ndikimi i tij në krimin e organizuar.

Në ditët e sotme, krimi kibernetik është larg nga hakerat që luftojnë me sistemet kompjuterike vetëm për argëtim ose për administrim të dhënash. Rritja e ekonomisë dixhitale ndryshoi plotësisht skenën kriminale ku qasja në asetet e ruajtura në sistemet e kompjuterit bëhet objektiv i krimit. Mundësia e fitimit të lartë e kombinuar me rreziqe praktikisht shumë të ulëta, i bënë rrjetet dixhitale një mjedis tërheqës për lloje të ndryshme të aktiviteteve kriminale. Krimi i organizuar në të kaluarën kishte gjetur një mjedis të sigurt në vendet me qeveri të dobëta dhe regjime politike të paqëndrueshme. Sot, krimi i organizuar përdor përparësitë e juridiksioneve kombëtare me korniza ligjore jo të duhura dhe aftësi të dobëta teknike për të luftuar krimin kibernetik.[10]

Historikisht, krimi i organizuar tradicional dhe krimi kibernetik kanë qenë dy degë të veçuara. Ekziston një shqetësim kryesor që vjen referuar vlerësimit tëEuropol 2017, “Mbi Kërcënimet e Krimit të Organizuar”, ku krimi i organizuar së fundmi është bërë dixhital, duke zhdukur dallimet origjinale midis këtyre dy kategorive. Të gjitha mënyrat e mundshme të krimit kibernetik, duhen marrë në konsideratë në krimin e organizuar si dronët, pajisjet gjurmuese, hakerimi, komunikimi i koduar etj. Ky është një

10 “Cybercrime and Organized Crime”, Vaclav Jirovsky, Czech Technical University in Prague https://www.firstlinepractitioners.com/cybercrime-and-organized-crime/

zhvillim që agjencitë e zbatimit të ligjit duhet ta njohin dhe ta trajtojnë mbi baza ndërkombëtare.[11]

Krimi kibernetik, sot është shëndëruar në një krim aq popullor dhe potencialisht fitimprurës saqë rrjetet e mirë organizuara të kriminelëve kibernetikë punojnë në bashkëpunim për të kryer grabitje masive nëpërmjet internetit. Këto organizata të krimit të organizuar kibernetik janë grupe hakerash, programuesish dhepërdorues të tjerë të teknologjisë që kombinojnë aftësitë dhe burimet e tyre për të kryer krime të mëdha që në forma të tjera nuk mund të ishin të mundshme.[12]

Grupet e organizuara të krimit kibernetik mund të shfaqen si në struktura të vogla por edhe në grupe tëmirë organizuara të lidhura në mënyrë rastësore por edhe me strukturë të mire përcaktuara; disa grupe veprojnë në formën e organiztatave kriminale, me drejtues dhe anëtarë që plotësojnë role specifike funksionale.

Organizatate krimit kibernetik vazhdojnë të përshtaten, duke gjetur mënyra të reja për të shfrytëzuar të dhënat personale të përdoruesve ose skedarët e ndjeshëm të biznesit. Vetëm gjatë vitit të kaluar, ka pasur një rritje të konsiderueshme të krimit kibernetik, të cilin shumë ekspertë ia atribuojnë pandemisë COVID-19. Shumë mashtrues kompjuterikkanë përfituar nga pasiguritë në periudhën e pandemisë, së bashku me dëshirën e publikut për informacion, duke dërguar përditësime të rreme për COVID-19,bashkë me software të krijuara për të dëmtuar ose për të marrë informacione të paautorizuara në kompjuterat personale. Shumë nga këto sulme kanë ardhur nga organizata të krimit kibernetik.[13]

4. Llojet e krimit të organizuar kibernetik

Ashtu si në krimin e organizuar tradicional, grupet e krimit të organizuar kibernetikë priren të drejtohen nga një lider kriminel që ka idetë, ndikimin dhe kontaktet për të kryer mashtrime dhe hakerime komplekse, me shtrirje të gjerë. Bosët e krimit kibernetik po bëhen gjithmonë e më të aftë në aktivitetet e tyre të paligjshme.[14]

11 Po aty

12 UNODC Unitet Nacions Office on Drugs and Crime “Criminal groups engaging in cyber organized crime”https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime.

13 Po aty

14 . Kjo është pohuar nga shkrimtari i teknologjisë Steve Ranger në artikullin e tij në ZDnet.com,

Por cili është saktësisht kërcënimi i krimit të organizuar kibernetik për qeveritë, bankat dhe korporatat e tjera të mëdha? Ndër llojet më kryesore të organizatave kriminale kibernetike dhe teknikat e tyre të shfrytëzimit, përmendim:[15]

Hakerimi (Hacktivists):[16] Disa grupe kriminelësh kibernetikë udhëhiqen nga një axhendë e caktuar politike ose sociale. "Hakerat" priren të jenë më të interesuar të vendosin në vështirësi kompanitë ose të publikojnë të dhëna të caktuara dhe zakonisht nuk janë të interesuar të grabisin paratë si objektiv apo asetet e tyre.

Terrorizmi: Kërcënimi i terrorizmit u rrit ndjeshëm pas sulmeve të 11 Shtatorit në SHBA. Fatmirësisht, shumica e organizatave terroriste nuk kanë njohuri teknike dhe burime për të kryer sulme të mëdha kibernetike. Sipas Projektit Ndërkombëtar të Rregullimit të Terrorizmit Kibernetik, krimi kibernetik terrorist tenton të përfshijë kryesisht publikimin e propagandës, fushatave psikologjike (të tilla si prerja e kokës dhe rregjistrimi i tyre në video), inteligjencës, shkëmbimin e informacionit dhe komunikime të tjera.

Hakerat e mbështetur nga shteti: Spiunazhi vazhdon të jetë i përhapur në botën moderne. Historia e kohëve të fundit është e mbushur me shembuj të fushatave të supozuara të hakerave të mbështetura nga shteti. Hakerimi i"*The Stuxnet worm hack*" i viteve 2000 dyshohet se u zhvillua nga SHBA dhe aleatët e saj për të ndërprerë programin bërthamor të Iranit. Kina është akuzuar për spiunazh dixhital që përfshin sekretet industriale të SHBA-ve. Në vitin 2020, hakerët e supozuar të mbështetur nga qeveria ruse, iu qasen qeverisë amerikane dhe rrjeteve të korporatave duke shfrytëzuar softuerin e prodhuar nga "*SolarWinds"*.

Kërcënimet e brendshme: Organizatat kriminale gjithashtu mund të synojnë të shantazhojnë edhe personat brenda organizatës, të cilët disponojnë informacione që të tjerat nuk i kanë. Qëllimi është të merren sekrete të koorporatës, të dhëna konfidenciale, fjalëkalime dhe lloje të tjera aksesi në rrjete të sigurta që mund të rezultojnë në vjedhjen e parave ose informacionit.

Linjat e paqarta: Si në cdo fushë tjetër, gjithmonë është e vështirë një ndarje strikte lidhur me krimet e konsumuara. Shumë grupe të organizuara të krimit kibernetik marrin pjesë në hakerimin e "të gjitha sa më sipër". Një organizatë terroriste, për shembull, mund të punësojë individë me njohuri

"Krimi kibernetik dhe lufta kibernetike: Udhëzuesi i një vëzhguesi për grupet që synojnë t'ju marrin".

15 University of North Dacota, What Is Organized Cyber Crime? https://onlinedegrees.und.edu/blog/organized-cybercrime-overview/

16 Një person që fiton akses të paautorizuar në skedarët ose rrjetet kompjuterike me qëllim që të çojë më tej qëllime sociale ose politike.

teknologjike për të rekrutuar anëtarë të rinj, për të drejtuar fushata hakerimi dhe për të vendosur një fushatë "phishing"[17] ose sulm ransomware[18] për të marrë informacione të ndjeshme të sigurisë kibernetike dhe për të financuar operacione terroriste.

Përfituesit ende mbretërojnënë botën e krimit kibernetik. Qendra Europiane kundër Krimit Kibernik në Europol, ka publikuar vlerësimin e saj në lidhje me Ransomware, si një lloj virusi kompjuterik me një rritje eksponenciale në Bashkimin Europian gjatë dy viteve të fundit. Në këtë teknikë, viktimat mbyllen jashtë kompjuterave të tyre, derisa të paguajnë një shpërblim në kriptomonedhë.Dhe, sigurisht, organizatat tradicionale të krimit kanë gjetur mënyra të teknologjisë së lartë për të trafikuar produktet dhe shërbimet e tyre të vjetra.

Interneti ofron anonimitet dhe anonimiteti krijon vese, thotë Maxwell D. Marker, Shefi i seksionit të krimit të organizuar trans-nacional të FBI-së[19]. Si rezultat, kartelet e drogës, shërbimet ilegale të lojërave të fatit, zhvatësit dhe rrjetet e prostitucionit shesin mallrat e tyre në internet dhe po aty pastrojnë paratë përmes mjeteve dixhitale.

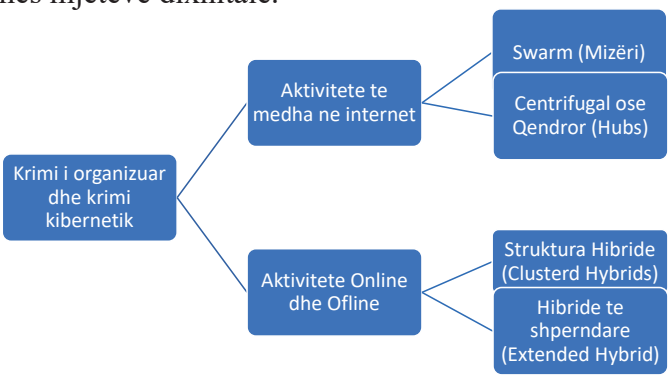

Figura 1: Llojet e grupeve kriminale që përfshihen në krimin e organizuar kibernetik[20]

17 Një organizatë apo individ përdor "Phishing" ('peshkimin') nëse është duke u përpjekur në mënyrë të paligjshme të marrë informacione të ndjeshme personale nga si: ID, fjalëkalimin, numrat e llogarisë bankare, numrat e kartës së kreditit etj

18 Ransomeware është një lloj virusi i cili kufizon qasjen në sistemin kompjuterik që ai infekton, dhe i kërkon një shpërblim krijuesit të viruseve në mënyrë që të heqë këtë kufizim.

19 Në një artikull të revistës së Shefit të Policisë, "Krimi i organizuar ka shkuar në teknologjinë e lartë".

20 UNODC Unitet Nacions Office on Drugs and Crime "Criminal groups engaging in cyber organized crime" https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime.

5. Luftimi i krimit kibernetik

Krimi kibernetik është mbas shumicës së sulmeve kibernetike sot, dhe ky është një krim po sjell të ardhura gjithmonë nërritje. Nevoja për barazimin dhe sistematizimin në nivel global të normave materiale dhe procedurale nga fusha e krimit kompjuterik dhe provave elektronike, e gjejmë edhe në Konventën për krimin kompjuterik të Këshillit të Evropës ose siç njihet ndryshe "Konventa e Budapestit". Edhe pse më parë ka pasur përpjekje për definimin e normave materiale që e rregullojnë bashkëpunimin juridik ndërkombëtar, megjithatë Konventa, për nga përfshirja e gjerë, fleksibiliteti dhe mundësia për ratifikim të lehtë në legjislacione të brendshëm edhe pse fillimisht e dedikuar për vendet evropiane, u bë mekanizëm për komunikim të lehtë ndërmjet vendeve nga e gjithë bota.[21]

Me Konventën për krimin kompjuterik më vonë u ndërlidhën edhe Konventa për mbrojtjen e të dhënave personale gjatë procesit të automatizuar për përpunimin e të dhënave personale me Protokollet shtesë për qarkullim të autorizuar të të dhënave personale jashtë vendit, Protokolli shtesë i Konventës për krimin kompjuterik për mbrojtje nga racizmi dhe ksenofobia, Konventa për mbrojtjen e fëmijëve nga keqtrajtimi seksual dhe Direktivat e BE-së.[22]

Këshilli i Evropës e miratoi Konventën për krimin kompjuterik në Budapest më 23.11.2001. Gjithsej 58 vende e kanë nënshkruar Konventën, prej të cilave 28 me ratifikim. Konventa u ratifikua nga ana e vendit tonë meLigj nr.8888, datë 25.04.2002.

Konventa përmban norma materiale, procedurale dhe norma për bashkëpunim ndërkombëtar. Dispozitat nga fusha e të drejtës materiale kanë të bëjnë me: hyrjen e paligjshme, interceptimin e paligjshëm, interferencën e të dhënave, interferencën e sistemeve, keqpërdorimin e pajisjeve, falsifikimet e lidhura me kompjuterët, mashtrimet e lidhura me kompjuterët, veprat penale të lidhura me pornografinë e fëmijëve, veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të të drejtave të tjera të lidhura me të.

Megjithatëkjo konventëfunksionon vetëm në qoftë se ka marrëveshje nderkombëtare për ta berë këtë. Arsyeja kryesore pse krimi kibernetik është kaq efektiv sot,është se ka vende që sigurojnë "strehë të sigurt" nga e cila kriminelët kibernetike mund të veprojnë.

Struktuart e krijuara në nivel ndërkombëtar të cilat bashkojnë qeveritë,

21 https://www.osce.org/files/f/documents/a/a/121225.pdf

22 Po aty

biznesin ndërkombëtar dhe organet e ruajtjes së rendit, përfshirë edhe Interpolin, të specializuara në luftën kundër krimit kibernetik në shkallë globale duhet të rrisin ndërveprimin e tyre me qëllim që ti përshtaten zhvillimit të vrullshëm të krimit të organizuar kibernetik.

Rritja e efikasitetit të njësive të krimeve kibernetike realizohet edhe nëpërmjet: rritjes së numrit të hetimeve të veprave penale të lidhura me krimet kibernetike; rritjes së numrit të hetimeve të rasteve të abuzimit të të miturve përmes internetit; si dhe rritjes së numrit të hetimeve parandaluese të krimeve kibernetike.

Konkluzione

Për një luftë sa më efikase ndaj krimit të organizuar dhe atij kiberentik, jo vetëm në nivel kombëtar por dhe në atë ndërkombëtar do të veçonim:

Objektivi i modernizimit duhet të jetë i pandashëm për çdo strategji që ka të bëjë me krimin e organizuar dhe kibernetik, së bashku me trajnimin e vazhdueshëm që duhet t'i jepet stafit për përdorimin e pajisjeve apo programeve më të reja.

Përfshirja e elementeve të luftës kundër promovimit të terrorizmit, kërcënimeve kibernetike dhe gjuhës së urrejtjes që përhapet në internet. Frymëzim i rëndësishëm për këtë çështje mund të jenë veprimetë ndërmarra nga disa rajone policie në Mbretërinë e Bashkuar që kanë krijuar forca të specializuara që veprojnë posaçërisht për të kontrolluar përmbajtjen në media, gjuhën e urrejtjes, promovimin e terrorizmit ose kërcënimet kibernetike.

Në vendin tonë të kryhet një reformë gjithëpërfshirëse dhe jo e copëzuar e institucioneve që kanë lidhje të drejtëpërdrejtë me luftën kundër krimit të organizuar, përfshirë Shërbimin e Policisë Gjyqësore; Të rritet bashkëpunimi dhe bashkërendimi i veprimeve midis Policisë së Shtetit, Shërbimit Informativ Shtetëror, Prokurorisë, Drejtorisë së Përgjithshme për Parandalimin dhe Pastrimin e Parave, Drejtorisë së Doganave dhe Tatimeve;

Të zhvillohen kapacitetet profesionale nëpërmjet trajnimeve të ndryshme, garantimit të qëndrueshmërisë në punë të specialistëve, përzgjedhjes së individëve mbi bazë merite, integriteti moral dhe shoqëror, dhe jashtë konfliktit të interesit;

Të mbështeten strukturat kundër krimit të organizuar në aspektin financiar dhe dhënien e një statusi preferencial me ligj;

Të rritet numri i konfiskimeve të të ardhurave të paligjshme.

Të rishikohen dhe zhvillohen kurrikulat mësimore. Studimi i krimit të organizuar të mos mbetet prerogativë vetëm e fakultetit të drejtësisë, por të përfshihet edhe në fakultetin e shkencave sociale, fakultetin ekonomik, dhe në fakultetin e shkencave të natyrës (departamenti i informatikës);

Të rritet ndërgjegjësimi publik mbi rrezikshmërinë e krimit të organizuar, si dhe rolin e përgjegjësinë e gjithsecilit në luftë kundër tij;

Bibliografi

1. Kushtetuta e Republikës së Shqipërisë
2. Kodi Penal i Republikës së Shqipërisë
3. Ligji nr. 9284 datë 30.09.2004 "*Për parandakimin dhe goditjen e krimit të organizuar*"
4. Ligj nr. 8920, datë 11.7.2002 Për ratifikimin e "*Konventës së Kombeve të Bashkuara kundër krimit të organizuar ndërkombëtar*" dhe dy protokolleve shtesë të saj
5. Elezi I, "*Vështrim mbi zhvillimet e legjislacionit penal shqiptar kundër krimit të organizuar" në "Gjendja e krimit të organizuar në Shqipëri, Kosovë, Mal të Zi, Maqedoni si dhe problemet që lidhen me të*" Tiranë, Dhjetor 2002.
6. Hoxha.D, Kaçupi.S, Haxhia.M "*E Drejta Penale, Pjesa e Përgjithshme*", Botimet Jozef, Durrës 2018, fq 482
7. Zhilla.F, Lamallari. B, Raport "*Vleresimi i riskut të krimit të organizuar në Shqipëri*", Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015,
8. Strategjia ndërsektoriale e luftës kundër krimit të organizuar, trafiqeve dhe terrorizmit, VKM 179, Gusht 2008, fq 6

"Cybercrime and Organized Crime", Vaclav Jirovsky, Czech Technical University in Prague https://www.firstlinepractitioners.com/cybercrime-and-organized-crime/

UNODC Unitet Nacions Office on Drugs and Crime "Criminal groups engaging in cyber organized crime" https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-

organized crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime.

University of North Dacota, What Is Organized Cyber Crime?

https://onlinedegrees.und.edu/blog/organized-cybercrime-overview/

UNODC Unitet Nacions Office on Drugs and Crime "Criminal groups engaging in cyber organized crime" https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime.

TË HETOSH KORRUPSIONIN DHE KRIMIN EKONOMIK NËPËRMJET SIMULIMIT TË NJË AKTI KORRUPTIV. KUSHTET, KËRKESAT LIGJORE DHE STANDARDET E GJEDNJ-SË.

ELIORA ELEZI[1]

SUELA XHANI[2]

Abstract

Korrupsioni është një fenomen kompleks, shumëdimensional i cili krijon pasoja në disa nivele të shoqërisë. Ai paraqet rrezik të shtuar në zhvillimin ekonomik, politik dhe në tërësi të gjithë marrëdhënieve demokratike bazë të një shteti. Ky deformim kërcënon vlerat etike e profesionale dhe rregulluese të funksionimit jo vetëm të veprimtarisë publike por edhe në aspektin privat tregtar. Në këto lloj krimesh, hetimi paraqet vështirësi sepse nuk kemi një vendngjarje klasike dhe gjurmët nuk gjenden lehtë. E kategorizuar si një krim "pa viktima" dhe "pa dëshmitarë", raportimi i tyre është i rrallë, përsa kohë ligji ndëshkon te dyja palët si mitëdhënësin dhe mitëmarrësin. Përdorimi i hetimit tradicional dhe instrumenteve të sanksionuar në legjislacionin procedurial penal, shpesh nuk jep rezultat. Në këto kushte ndryshimet e ardhura si pasoje e përsosjes së kryerjes se këtyre krimeve dhe raportimeve të ulta kanë sjellë nevojën e adoptimit të metodave të reja të hetimit. Aplikimi i teknikave speciale të hetimit sikur mund të jenë veprimet simuluese ndikuan në rritjen në mënyrë efikase të luftës kundër korrupsionit apo krime të tjera serioze. Në vetvete teknikat speciale te hetimit për shkak të natyrës përfshirësëe të tyre në jetën private të individit, kërkohen të përdoren si mjet i fundit dhe brenda një kuadri strikt rregullues, në mënyrë

1 Magistrate-Prosecutor in Kruja District Court email : elioraelezi@yahoo.com.

2 Magistrate-Judge of First Instance in Saranda District Court email suelaxhani88@gmail.com.

që mbledhja e provës të jetë e ligjshme dhe e përdorshme. Njohja më e mirë e këtyre metodave shfaq një rëndësi të veçantë për institucionet ligjzbatuese por edhe për individin që mund të rrezikohet ti cenohet jeta private nga përdorimi i paligjshëm i tyre.

***Fjalët kyçe**: korrupsioni, metodat speciale te hetimit, veprimi simulues, hetim proaktiv, prova të papërdorshme*

Investigating corruption and economic crimes through simulating an corruptive act. Conditions, law requirements and ECHR standards.

Eliora ELEZI

Suela XHANI

Corruption is a complex, multidimensional phenomenon, which creates consequences at several levels of society. It poses an added risk to the economic, political and overall development of a country basic democratic relations. This distortion, threatens the ethical, professional and regulatory values of the functioning not only of the public activity but also in the private commercial aspect. In these types of crimes, the investigation presents enormous obstacles because it lacks a classic crime scene and the traces are not easily found. It is also categorized as a "victimless" and "witness less" crime, and because of this, their reporting is rare, as long as the law punishes both parties; the bribe-giver and the bribe-taker. The use of traditional investigation methods and instruments in criminal procedural legislation often does not bring results. In these conditions, as the methods used from the wrongdoers are getting better, and because of the low reporting, the need to adopt new methods of investigation is crucial. The application of special investigative techniques, such as the simulation of an corruptive act, has effectively enhanced the fight against corruption or other serious crimes. By themselves special investigative techniques due to their intrusive nature in the private life of the individuals, are required to be used as a last resort and within a strict regulatory framework, so that the collection of evidence is lawful and also admissible in the court of law. Better knowledge of these methods shows a special importance for law enforcement institutions but

also for the individual, whose privacy may be endangered by their illegal use.

Key words; *corruption, special investigative techniques, corruptive simulation act, proactive investigations, inadmissible evidence.*

Kreu I

1. 1 Kuptimi krimit ekonomik. Rëndësia dhe efektit e tij në shoqëri.

Termi kriminalitet ekonomik për shkak të dimensionit që ka nuk mund të përkufizohet brenda një definicioni shterues. Doktrina të ndryshme penale juridike e lidhin atë në disa raste nën një kuptim te ngushtë me veprime të kundraligjshme, shoqërisht të rrezikshme që mund ti shkaktohen pronës, por gjithsesi ky interpretim nuk është i mjaftueshëm. Në këtë këndvështrim konsiderohen veprimet e mosveprimet të personave fizike apo juridike në sferën e qarkullimit financiar dhe tregtar të drejtuar kundër sistemit ekonomik pavarësisht nga statusi ligjor i pronës që janë të inkriminuar me ligj penal ose ligje të tjera si vepra të ndaluara e të dëmshme shoqërore.[3]

Duke qenë një fenomen i cili nuk njeh kufi, hera herës shfaqet si bashkëshoqëruese e një sërë krimesh të organizuara si produkt i tyre apo i marrëdhënies që synohet të cenohet. Kompleksiteti shfaqet se krimi ekonomik nuk është vetëm një kategori juridike por ndërthur elemente social-ekonomike me ndikim të pashmangshëm të bazat e shtetit të së drejtës.

Megjithatë është e mirëpranuar se krimet ekonomike mbulojnë një gamë të gjerë veprash, duke përfshire mashtrimin, korrupsionin, pastrimin e parave, krimet kundër pronës edhe asaj intelektuale apo dhe krimin mjedisor. Hetimet penale si: trafikimi i lëndëve narkotike, i qenieve njerëzore apo dhe më gjerë në krimet serioze si: aktet terroriste zakonisht përfshijnë si pjesë të tyre dhe elemente të krimit ekonomik.[4]

Një nga veprat penale me të rëndësishme për tu analizuar në kuadër të krimit ekonomik është padyshim korrupsioni, i cili në vetvete cenon shoqërinë dhe zhvillimin e saj në shumë dimensione. Edhe pse ka ekzistuar

3 Armand Krasniqi, "Ekonomia dhe kriminaliteti ekonomik" January 2003 Conference: Revista "E drejta / Law" Universiteti i Prishtinës - Fakulteti Juridik: Volume: 4/2003.

4 https://wwweurojust.europa.eu/crime-types-and-cases/crime-types/economic-crimes, aksesuar dt .05.6.2022.

që me gjenezën e shoqërisë kjo nuk zbeh faktin se kërcenon parime bazë si: barazia, paanësia, merita, integriteti dhe në tërësi gjithë themelet e shtetit të së drejtës. Për sa më sipër do të analizohet kuadri rregullues material dhe procedural për të kufizuar sa më shumë të jetë e mundur këtë fenomen në shoqëri.

1.2 Vepra penale e korrupsionit. Kuadri ligjor dhe definicioni i tij.

Fjala "korrupsion" vjen nga fjala latine "corrumpere", që do të thotë "thyej"ose "shkatërroj". Në këtë këndvështrim një akt korruptiv, pikë së pari cenon, thyen bazat etike dhe integritetin moral të një marrëdhënie të mbrojtur nga ligja. Nga ana tjetër, 'ryshfeti - mita në rumanisht (nga fjala sllave "mito") do të thotë para ose mallra të marra prej dikujt ose të dhëna dikujt në shkëmbim të dashamirësisë së atij personi dhe që e bën atë të kryejë një detyrë të punës ose të kryejë një paligjshmëri në favor të atij që e paguan mitën ose që ofron mallrat'.[5]

Ndërsa sipas një këndvështrimi tjetër korrupsioni mund të trajtohet si një marrëveshje e veçantë (pactum sceleris) mes një funksionari publik apo subjekteve te tjera të specifikuara dhe një subjekti privat, përmes të cilit, i pari pranon nga i dyti, për një sjellje që lidhet me detyrën e tij, një shpërblim që nuk i takon.[6]

Fjalori "Black Law" jep një përkufizim ligjor më të gjerë të korrupsionit: *" një veprim që bëhet me synimin për të dhënë disa avantazhe që nuk përputhen me detyrën zyrtare dhe të drejtat e të tjerëve. Akti i një zyrtari ose personi kujdestar që në mënyrë të paligjshme dhe të gabuar përdor pozicionin ose karakterin e tij për të nxjerrë përfitim për vete ose për një person tjetër, në kundërshtim me detyrën dhe të drejtat e të tjerëve"*[7].

Parashikime ligjore mbi definicionin e korrupsionit gjenden të sanksionuara e dhe në një sërë aktesh të legjislacionit tonë të brendshëm, për të cilat diferencat në trajtim nuk janë shumë të qenësishme[8] për tu analizuar.

---

5 Akademia Rumune, 'Micul Dictionarul Academic/ Fjalor i Vogël Akademik', volumi I, Shtëpia Botuese Univers Encinclopedic, Bukuresht, 2001. cituar ne http://cristidanilet.wordpress.com.

6 https://dizionari.simone.it/3/pactum-sceleris?hl=Pactum%20sceleris.

7 Black's Law Dictionary /ed. Bryan A. Garner. – 7th ed. – St. Paul: west Group, 1999.

8 Sipas ligjit nr. 8635, dt .06.07.2000 "*Për ratifikimin e konventës civile për korruspionin*," n. 2, fjala "*korrupsion*" merr kuptimin e *të kërkuarit, ofrimit, dhënies ose pranimit drejtpërdrejt ose nëmënyrë të tërthortë të një mitëmarrje ose çdo lloj tjetëravantazhi ose përfitimi që deformon kryerjen e çdo detyre osesjellje të kërkuar nga pranuesi i mitëmarrjes, për pasojë dhe të avantazhit e përfitimit të padrejtë.*

Korrupsioni është një krim që përfshin *dy subjekte*, të cilët janë pjesë esenciale e veprës penale. Më pas në varësi të këtij elementi dhe të sjelljes së tyre, e përkthyer në veprimtari të kundraligjshme në këndvështrim të faktit, bëjmë dallimin e korrupsionit aktiv (ai që korrupton) dhe pasiv (të korruptuarit). Megjithatë nga kryerja e veprës penale të korrupsionit të dy subjektet janë përfitues, i pari merr si pasojë një shpërblim, një veprim që lidhet me detyrën e të dytit.

Për t'u quajtur i kryer korrupsioni, mjafton që të jetë kërkuar, marrë apo premtuar përfitimi i padrejtë pavarësisht nëse është kryer apo jo sjellja e kërkuar në ushtrim të funksioneve.[9] Karakteristike dalluese për korrupsionin është se kërkimi apo marrja, ofrimi apo dhënia duhet të ketë një lidhje me detyrën që ai bën. Nuk kemi konsumim të veprës penale të korrupsionit në rast se subjekti pasiv merr shpërblim për të kryer një veprim që nuk lidhet me detyrën e tij.

Për t'u quajtur i kryer korrupsioni, nuk është e nevojshme që veprimi që kërkohet të kryhet të jetë i përfshirë në pushtetin e detyrave të funksionarit publik por mjafton që të jetë një veprim që kryhet nga zyra apo institucioni ku punon ky funksionar publik dhe ku ai mund të ketë akses.[10]

Në përgjithësi korrupsioni perceptohet vetën në sferën e marrëdhënieve juridike publike (kryesisht të administratës publike)[11] si objekt i cenuar nga veprimtaria e paligjshme dhe që ligja e merr në mbrojtje të posaçme për të ruajtur funksionimin e rregullt të tyre me korrektësi, integritet, paanësi dhe etikë. Në varësi të faktit nëse funksionari kryen veprime në ushtrim të detyrës sipas ligjit apo në kundërshtim më të, me qëllim përfitimin e padrejtë, mund të bëhet dallimi i marrëdhënies së mbrojtur nga ligja, nëse ky i fundit është i llogaritshëm në dëme materiale apo jomateriale. Do të quhen detyra në kundërshtim me funksionet e veta jo të vetëm ato që janë në kundërshtim me ligjin por edhe ato që edhe pse duken të rregullta, cenojnë parimin e korrektësisë apo barazisë, paanësisë. [12]

Gjejmë një përkufizim krejtësisht tjetër në ligjin nr. 9508 datë03.04.2006 "*Për bashkëpunimin e publikut në luftën kundërkorrupsionit"* që ngatërrohet me shpërdorimin e detyrës. N. 2 pika 4 përcakton se "*Praktikë korruptive*" është *çdo veprim osemosveprim, i kryer duke abuzuar me autoritetin publik, përsigurimin e përfitimeve të paligjshme për interesa privatë në dëm të interesave të shtetit apo të shtetasve.*

9 Gjykata e Kasacioni në Itali, Dhoma Penale *Seksioni* nr.I,Vendim nr. 4177, *datë* 4-2-2004 (ud. 27-10- 2003) rv. 227099.

10 Gjykata e Kasacioni në Itali, Dhoma Penale *Seksioni* nr.I,Vendim nr. 4177, *datë* 4-2-2004 (ud. 27-10- 2003) rv. 227100.

11 Kodi Penal I Republikës së Shqipërisë në një sërë veprash rregullon dhe korrupsionin privat .

12 Gjykata e Kasacioni në Itali, Dhoma Penale *Seksioni* nr.VI,Vendim nr. 3388, *datë* 23-1-2003

1.3. Përdorimi i teknikave tradicionale te hetimit ne veprim

Rreziku relativisht i ulët dhe fitimet e larta që lidhen me krimin ekonomik e bëjnë atë një aktivitet shumë tërheqës për krimin e organizuar. Si të tilla kjo veprimtari kriminale, me shumë gjasa, mund të shtrihet në më shumë se një shtet dhe mundësia që të ndiqen penalisht mund te jetë rezultativ vetëm përmes bashkëpunimit ndërkombëtar, për shkak të kompleksitetit të hetimeve të kërkuara.

Formacionet e krimit të organizuar që veprojnë në nivel transnacional shfrytëzojnë dhe ndryshimet në legjislacionet e shteteve të përfshira. Për nga natyra e krimit ekonomik shoqërohet dhe me perceptim të ulët të rrezikut nga ana e viktimave dhe mungesë të ndërgjegjësimit të tyre.

Dëmet e mëdha që i shkaktohen sistemit ekonomik-financiar të një shteti nga veprimtaria krimit ekonomik ka pasoja të konsiderueshme në funksionimin e tij (p.sh në shtyllën e të ardhurave në sigurimeve shoqërore) dhe mund të sjellin destabilizim deri në dështim total. Për këto arsye krimi ekonomik është një krim serioz që në shumë raste merr formë të organizuar dhe lind nevoja luftimit në aspektin ligjor penal të këtij fenomeni.

Përdorimi i teknikave tradicionale hetimore, për të luftuar krimin e organizuar ndërkombëtar në kohë, rezultoi e pamjaftueshme ose joefektive. Ndërsa vënia në zbatim i mjeteve të posaçme të hetimit, nga ana tjetër shfaqi mundësinë potenciale për cenimin e të drejtave themelore të njeriut. Balanca dhe ekuilibri i duhur mund të arrihet duke u mbështetur tek parimet bazë si: ligjshmërisë, kontrollit, interesit publik etj. Diskutimet mbi këto teknika shpesh here tejkalojnë planin juridik dhe shkojnë deri në atë politik dhe jo vetëm.

Megjithatë është tashme e pranuar se hetimi reaktiv, pra mbi bazën e ankesave, nuk është gjithmonë rezultativ,[13] sidomos në rastet kur mungojnë dëshmitarët ose janë pak të besueshëm. Për shume arsye, u kalua në hetimin proaktiv, i cili për nga natyra lejon organet proceduese të zbulojnë dhe ndalojnë shkelësit e ligjit gjatë kryerjes së veprave penale, duke mbledhur dhe prova mbi gjithë rrjedhën "*historike*" të krimit.[14]

(ud. 4-12-2002) rv. 224056.

13 Clive Harfield, "Pro-activity, partnership and prevention: the UK contribution to policing organised crime in Europe" The Police Journal (vol. 73, nr.2, 2000), fq.109.

14 Eliora Elezi "Teknikat speciale te hetimet. Veprimet simulese dhe agjenti infiltruar". Temë e mbrojtur nën udheheqjen e A. Xholi Shkolla e Magjistraturës viti 2017.

Kreu II

2.1 Simulimi i nje akti korruptiv, Kushtet kriteret e zbatimit.

Mënyra më efikase për të luftuar korrupsionin është përdorimi i teknikave speciale te hetimit dhe duke e hetuar në mënyrë më dinamike. Nuk mund të luftohet ky fenomen me kallëzime sporadike. Lufta kundër korrupsionit është e lidhur ngushtësisht me luftën kundër krimit të organizuar, trafiqeve të paligjshme e terrorizmit, që ngjallin shqetësim në komunitet. Parandalimi dhe reduktimi progresiv i korrupsionit kërkon forcimin e integritetit të organeve të ndjekjes penale. Rritja e treguesve nëpërmjet fuqizimit të kapaciteteve të hetimit të korrupsionit, evidentimit dhe dokumentimit sa më efektiv të hetimeve për korrupsion, krijimit të një sistemi të konsoliduar të dhënash në lidhje me regjistrimin e hetimeve, ndjekjes penale dhe dënimeve në fushën e korrupsionit, si dhe rritjes së besimit të publikut te strukturat e luftës kundër korrupsionit, janë pjesë përbërëse e luftës pa kompromis kundër korrupsionit.[15]

Sipas ligjit procedural penal shqiptar, operacionet e fshehta janë teknika të cilat në fakt janë ndarë në dy lloje, të ashtuquajturat veprime stimuluese, dhe e dyta e agjentit të infiltruar brenda strukturave të krimit të organizuar. Ato gjenden të rregulluara shprehimisht në nenet 294 / a dhe 294 / b të K.Pr.Penale. Metodat speciale të hetimit kanë për qëllim: **gjurmimin**, **identifikimin** dhe **dokumentimin** e veprimtarisë kriminale të të gjithë personave (korrierëve, blerësve, organizatoreve, financuesve etj.) dhe/ose organizatave kriminale të përfshira në trafikun e organizuar ndërkombëtar të lëndëve narkotike,[16] por jo vetëm.

Përdorimi i këtyre teknikave synon **theksimin e përgjegjësisë së personit** të akuzuar, me kusht të domosdoshëm për lejimin e aplikimit, ekzistencën paraprake të provave mbi fajësinë. Pra në këto raste, oficeri i policisë gjyqësore duhet të jetë përballë një **oferte ekzistuese,** e cila sjell dyshimin për kryerjen e në krimi dhe që simulohet prej tyre për të vërtetuar kryerjen e saj nga i dyshuari. Oficeri, agjenti i policisë, për aq sa të jetë e mundur nuk duhet të sillet në mënyrë aktive, por duhet të shërbejë si "*katalizator*", duke krijuar mundësinë e sigurimit të objekteve të autorizuara, për të kryer krimin

15 Pika 2 e Vendimit Nr. 387, datë 02.05.2013 "Për miratimin e Rekomandimeve në Luftën kundër Kriminalitetit për vitin 2013 ".

16 Udhëzimi I Prokurorit të Përgjithshëm dhe Ministrit të Rendit " Për përdorimin e metodave speciale të hetimit të krimeve kundër drogës" që I përket muajit prill të vitit 2003.

nga kryerësit e tyre.[17] Ata duhet të jenë në gjendje të provojnë se i pandehuri ishte i prirur për të kryer krimin, edhe nëse nuk do të kryhej operacioni i fshehtë.

Në nenin 294/a te K.Pr.Penale përcaktohet që oficeri dhe agjenti i policisë gjyqësore ose personi i autorizuar prej tyre mund të ngarkohen për simulimin e një akti korruptiv. Këto veprime bëhen me autorizim të prokurorit që kontrollon hetimet ose të prokurorit që ka në juridiksion territorin ku do të zhvillohet veprimi. Sikurse shihet nga formulimi i dispozitës simulimi i një akti korruptiv mund te kryhet nga : a) oficeri ose agjenti i policisë gjyqësore b) personi i autorizuar prej tyre[18].

Për efekt krahasimi i referohemi dhe në këtë rast rregullimit të kësaj teknike në Kosovë, ku shprehja "*simulim i veprës penale-mitë*" nënkupton aktin i cili është I ngjashëm sikurse vepra penale lidhur me mitës, përveç që kryhet me qëllim të mbledhjes së informatave dhe provave në procedurën penale.[19]

Në praktikën gjyqësore, shpesh herë krijohet konfuzion në përdorimin e termit person i

"infiltruar" [20] edhe kur I referohen subjekteve që kryejnë një veprim simulues, ndryshe nga teknika me të njëjtën emër e parashikuar nga neni 294/ b i K.Pr.Penale " *agjent i infiltruar*". Në fakt do të ishte me e saktë përdorimi I termit personi nën mbulim, i cili është një term më gjithëpërfshirës.

Përveç përcaktimit të subjektit, në një rast gjykata i ka dhënë peshë dhe procedurës të brendshme administrative mbi mënyrën e lëvrimit të shumës (objekt simulimi). Ky element nuk lidhet më kushtet thelbësore të simulimit të një akti korruptiv. Ndërsa gjykata ka kthyer çështjen për rigjykim duke

17 Bruce Hay, "Sting Operations, Undercover Agents, and Entrapment", Missouri Law Review (Vol. 70,Nr.2, 2005) fq. 388. Aksesuar në datë 02 qershor , në adresën < http://scholarship.law.missouri.edu/mlr/vol70/iss2/2/>.

18 Vendim i Gjykatës së Apelit Tiranë, me Nr.519, datë 11 Maj 2012 citoj :" *Për shkak të situatës së krijuar, e dëmtuara me datë 27.04.2011 ka pranuar të bashkëpunojë me opgj dhe kryerjen e veprimeve simuluese. Për këtë qëllim me datë 28.04.2011 të dëmtuarës i është dhënë shuma 2000 euro në kartëmonedha të prerjes 100 euro, të cilat janë rregjistruar në procesverbalin përkatës."*

19 Hajrija Sijerçiq – Çoliq, Haris Haliloviq E drejtë procedurës Penale në vështrim të posacëm në procedurën penale në Kosovë përktheu nga kroatishtja: Mustafë Reçica (Prishtine, 2007) fq .136.

20 Vendimi I Gjykatës së Lartë Nr.159, datë 20 Korrik 2016, ku shprehet se*:" Shërbimet e policisë gjyqësore kanë kërkuar lejimin e veprimeve simuluese, duke përdorur një agjent të infiltruar të policisë si dhe lejimin e përgjimit të numrit të telefonit 0682571964 të personit të dyshuar me emrin Genti" .*

arsyetuar: *"Gjykata e Apelit nuk ka arsyetuar gjithashtu në lidhje me efektet që passjell fakti që shuma e të hollave është dhënë* ***personit të infiltruar*** *nga oficeri i policisë gjyqësore në mënyrë private pa miratimin e shefit të Sektorit Kundër Krimit Financiar dhe pa u tërhequr nga fondi i veçantë i Drejtorisë së Policisë së Qarkut Korçë*[21] *"*

Si në të gjitha rastet kur kemi një veprim simulues, edhe në rastin e simulimit të një veprimi korruptiv, **kërkohet të mos provokohet**, ndryshe prova nuk është e përdorshme në procesin penal. Ky parashikim mbron subjektet, të cilat mund të tundohen nga oferta, vlerësuar rrethanave të kryerjes së saj, nëse nuk kishin asnjë predispozitë të mëparshme për të kryer veprën penale. Për sa më sipër në një çështje gjyqsore është arsyetuar mbi këto elemente si më poshtë vijonn : *"Nga analiza e këtyre dëshmive dhe akteve të ndodhura në dosje rezulton se përfundimi i Gjykatës së Shkallës së parë është i gabuar, pasi fakti i pretenduar nga organi i akuzës nuk provohet. Kjo për arsye se, në gjykim nga thëniet e dëshmitarëve del se i pandehuri nuk ka kërkuar ndonjë shumë parash. Ka qenë vetë kallëzuesi, i cili është interesuar dhe ka kërkuar të dijë se sa duhet të paguajë për lidhjen e kontratës. Pikërisht, kjo ka qenë arsyeja që ai ndonëse në aktin korruptiv simulues ka marrë shumën prej 3.500.000 lekësh të vjetra, ai ka ndarë 1.500.000 lekë të vjetra dhe këtë shumë pa ia kërkuar njeri e ka lënë mbi tavolinë. Pra, shuma e lekëve objekt vepre të mundshme penale, përcaktohet nga bashkëpunuesi dhe jo nga autoriteti i procedimit, siç thotë ligja apo nga subjekti i procedimit "mitë kërkuesi" si dhe kjo shumë parash lihet në mënyrë të padukshme dhe e pa kërkuar nga subjekti i proceduar."* [22]

Që të jepet autorizim për simulim të një akti korruptiv duhen plotësuar këto kushte: të jetë regjistruar procedimi penal; të ketë prova që subjekti i ngarkuar me një funksion shtetëror kërkon shpërblim për kryerjen ose moskryerjen e një veprimtarie të caktuar.

Gjykata e Lartë në një çështje të saj ka sqaruar përdorimin e kësaj teknike që mbart dhe vlera doktrinale shpjeguese mbi procedurën dhe vlefshmërinë e provave të marra. Kolegji Penal i Gjykatës së Lartë,[23]në çështjen penale ndaj të gjykuarve V.E., K.Ç. dhe V.A arsyeton: "*Në lidhje me veprimet simuluese Kodi i Procedurës Penale në nenin 294/a-3 të K.Pr.Penale parashikon se: "3. Nuk duhet provokuar një akt kriminal, duke shtyrë një person të kryejë*

21 Vendimi I Gjykatës së Lartë Nr. 205, datë 29 Tetor 2014.

22 Gjykata e Rrethit Gjyqësor Tiranë me Vendimin me Nr. 550, datë 06 Maj 2013 e shpall fajtor, Gjykata e Apelit Tiranë me Vendimin me Nr. 262, datë 17 Mars 2014, ka vendosur pushimin e çështjes dhe Gjykata e Lartë me Vendimin Nr.216, datë 16 Dhjetor 2015, e kthen për rigjykim.

23 Vendimi i Gjykatës së Lartë nr.85, datë 06 Mars 2013.

një krim, të cilin nuk do ta kishte kryer po të mos ishte ndërhyrja e policisë. Kur vërtetohet provokimi, rezultati nuk mund të përdoret". Përsa i takon veprimit simulues Kolegji Penal konstaton se ka pasur provokim nga ana e punonjësit të policisë që ka simuluar. Kështu agjenti me emrin fiktiv Luan Shehu me datën 14.10.2008 ka kontaktuar me shtetasin V.E. ku ka qenë i pranishëm edhe shoku i tij, V. A Gjatë bisedës shtetasi V.E. i sqaron personit të infiltruar të gjithë mekanizmin se si do ta çonte atë në Greqi, duke i thënë dhe sa do të paguante dhe njëkohësisht i ka marrë dhe numrin e pasaportës që kishte me vete. Rezulton se agjenti i infiltruar nuk ka asistuar në kryerjen e ndonjë ***vepre penale përpara provokimit që i ka bërë të gjykuarit V.E.****. Në lidhje me veprimet e simulimit, në çështjen* ***Ramanauskas kundër Lituanisë,*** *GJEDNJ[24] ka arritur në përfundimin se për të konstatuar nëse oficerët e policisë e kanë kufizuar veten për të* ***" hetuar veprimtarinë kriminale në thelb në mënyrë pasive",*** *nga ana e tyre* ***nuk duhet të kryen veprime aktive por duhet ta hetojnë veprimtarinë kriminale në mënyrë pasive. Rasti objekt shqyrtimi në GJEDNJ kishte të bënte me mungesën e provave më të hershme në kohë se veprimi i simulimit, që të krijonin dyshimin se personi do të kryente vepër penale pa qenë i ndikuar nga oficerët.*** *Kështu, edhe në rastin konkret agjenti i infiltruar nuk është mjaftuar në hetimin e veprimtarisë kriminale në mënyrë pasive, por ka kryer veprime aktive, duke i kërkuar pajisjen me vizë shengen falso, kundrejt shpërblimit. Nuk rezulton që agjenti të ketë konstatuar ekzistencën e ndonjë veprimtarie kriminale të kryer nga i gjykuari me persona të tjerë, ku ky agjent të ketë pasur rol pasiv*"

Përfundimisht shtetet me demokraci jo shumë të qëndrueshme, nevojitet të shtrihen hetimet kundër korrupsionit edhe në nivelet e mesme dhe të larta të administratës publike duke rritur numrin e hetimeve proaktive në luftën kundër korrupsionit.[25] Përdorimi sa më efektiv i teknikave speciale të hetimit

---

24 Në çështjen ***Ramanauskas kundër Lituanisë,*** **Aplikim nr. 74420/01, Vendim i Dhomës së Madhe të GJEDNJ-së, datë** 05 Shkurt 2008," *kërkuesi (që ushtronte funksionin e prokurorit) ishte kontaktuar me ndërmjetësinë e një të njohuri të tij, me një person që ishte agjent i fshehtë i policisë gjyqësore (shërbimi i luftës kundër korrupsionit), i cili i kishte kërkuar të pushonte hetimet për një person, kundrejt një ryshfeti në shumën 3,000 (tre mijë) dollarë amerikanë. GJEDNJ-a, duke gjetur shkelje të nenit 6/1 të Konventës (e drejta për një gjykim të drejtë), konsideroi se në rrethanat e ndodhjes së akti korruptiv, kur nuk kishte asnjë indicje të mëparshme që kërkuesi po kryente një akti korruptiv; kur ai nuk kishte kërkuar ryshfet për pushimin e akuzave ndaj një personi që po e hetonte; kur nuk e kishte kontaktuar asnjëherë as me telefon apo kërkuar ta takonte agjentin e policisë, por përkundrazi ishte ky i fundit që e kontakte shumë herë, duke i kërkuar me insistim që ta merrte ryshfetin dhe ta pushonte çështjen penale. Sipas GJEDNJ-së policia gjyqësore nuk kishte qëndruar pasive gjatë aktit kriminal, por e kishte nxitur dhe shtyrw atë, duke passjellë provokim të veprës penale."*

25 pika 2 ii) marrja e masave, Vendimit Nr. 387, datë 02.05.2013 " Për miratimin e rekomandimeve në luftën kundër kriminalitetit, për vitin 2013"

për sigurimin e provave dhe goditjen e korrupsionit, duhet të realizohet në përputhje me standardët e GJEDNJ-së.[26]

2. 2 Përdoshmëria / papërdoshmëria e provave të mara[27] nga përdorimi i teknikës speciale të hetimit, veprimeve simuluese. Standardet e GJEDNJ-së.

Neni 32/2 i Kushtetutës së Shqipërisë parashikon që asnjë person nuk mund të dënohet në bazë të dhënave të mbledhura në mënyrë të paligjshme. Sipas GJEDNJ-së, zbatueshmëria e nenit 6 mbulon procedimet në tërësi, duke përfshirë edhe ato që lidhen me marrjen e provave, rrjedhimisht përfshin procedimet hetimore dhe gjyqësore.[28]

Meqenëse operacionet nën mbulim, në thelb kanë natyrë invazive dhe sekrete, ekziston një rrezik potencial të ndërhyjnë dhe në të drejtën për jetë private sipas nenit 8 (1) KEDNJ-së (por jo gjithmonë[29]). Efektin që sjell provokimi ne provat e mara gjatë kryerjes së këtyre operacioneve, si dhe standardet i gjejmë dhe në vendimi gjyqësor të poshtë cituar: *"Ndërsa, rastet kur do të aplikohet "veprimi i simuluar" janë parashikuar në n. 294/a të K.pr.Penale. Kodi nuk e përkufizon veprimin e simuluar por, parashikon se, ky veprim nuk duhet të kaloje në "provokim[30]", duke shtyrë një person të kryejë një krim, të cilin nuk do ta kishte kryer, po të mos ishte ndërhyrja e policisë. Ky ndalim është i një natyre absolute dhe passjell papërdorshmërinë e rezultatit të arritur. Këtë qëndrim mban GJEDNJ, në çështjen Teixeira de Castro vs Portugalisë*."

Autoritetet publike duhet të autorizojnë, drejtojnë dhe mbikëqyrin përdorimin e metodave të fshehta[31] brenda qëllimit dhe diskrecionin që i jepet. Në mbrojtje nga veprimet arbitrare, mbikëqyrja e përdorimit të metodave

26 Eliora Elezi "Teknikat speciale te hetimet. Veprimet simulese dhe agjenti infiltruar". Temë e mbrojtur nën udheheqjen e A. Xholi Shkolla e Magjistraturës viti 2017.

27 Neni 152/1 i Kodit të Procedurës Penale " Çmuarja e provave është përcaktimi i vërtetësisë dhe i fuqisë provuese të tyre. Çdo provë i nënshtrohet shqyrtimit gjyqësor dhe nuk ka vlerë të paracaktuar. Gjykata i çmon provat sipas bindjes së formuar pas shqyrtimit në tërësi të tyre" .

28 Shih GJEDNJ, Engel dhe të tjerë kundër Hollandës, Aplikim Nr. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, datë 08 Qeshor 1976, pg. 82-83.

29 Shiko Lüdi kundër Zvicrës, Aplikim Nr.12433/86, datë15 Qershor1992.

30 Vendimi Nr. 287, datë 04 Korrik 2013 i Gjykatës së Rrethit Gjyqësor Elbasan.

31 Shih GJEDNJ, Kopp kundër Zvicrës, Aplikim nr. 23224/94, datë 25 Mars1998, dhe Taylor-Sabori kundër Mbretërisë së Bashkuar, Aplikim nr. 47114/99, datë 22 Tetor 2002.

të fshehta nuk duhet të jetë e pavarur[32]. Është e nevojshme të ekzistojnë nivele të miratimit dhe mbikëqyrjes që nuk e përjashtojnë njëra tjetrën. Pra të ketë një sistem gjithëpërfshirës dhe të fuqishëm për llogaridhënie dhe transparencë e cila mund të përfshijë më shumë se një nivel miratimi dhe më shumë se një mekanizëm mbikëqyrje.

Ndërsa për sa i përket ligjshmërisë dhe pranueshmërisë së provave të marra gjatë operacioneve të tilla, Gjykata ka qenë e prirur të vlerësojë kryesisht në përputhje me nenit 6 (për proces te rregullt ligjor) të Konventës[33]. Ajo vuri në dukje në këtë drejtim se përdorimi i metodave speciale të hetimit - në veçanti, hetimeve nën mbulim - nuk mund të shkelë në vetvete të drejtën për një proces të rregullt ligjor.[34] Administrimi i drejtë i drejtësisë ka një vend të rëndësishëm dhe nuk mund të sakrifikohet[35] për Gjykatën Evropiane të Drejtave të Njeriut e cila është shprehur se: "*interesi publik nuk mund të justifikojë përdorimin e provave të mara si rezultat i provokimeve të policisë, sepse kjo do të ekspozonte të akuzuarin në rrezik për t'u privuar përfundimisht e nga e drejta për një proces të rregullt ligjor që nga fillimi*"[36].

Në këtë rrethanë, dyshimi duhet të bazohet në prova konkrete që tregojnë hapat fillestare për kryerjen e veprës për të cilën akuzuari do të ndiqet më pas.[37] Gjykata gjithashtu kontrollon "nëse nuk ka prova që tregojnë se, pa ndërhyrje të tilla, vepra nuk do të ishte kryer" [38] Për gjykim të drejtë brenda kuptimi i nenit 6 të KEDNJ-së, "të gjitha provat e marra si rezultat i nxitje së policisë duhet të përjashtohet"[39].

Nuk është domosdoshme që agjenti të veprojë krejtësisht në mënyrë pasive agjenti, por sa më e madhe të jetë nxitja aq më shumë ka të ngjarë që gjykata të konsiderojë të papranueshme. Të gjitha provat në bazë të së cilave

32 Çështja GJEDNJ -së Malone kundër Mbretërisë së Bashkuar, Aplikim nr. 8691/79. datë 02 Gusht 1984.

33 Gjykata e Kasacioni në Itali, Dhoma Penale Seksioni nr.III,Vendim nr. 20238, nr. 38488, datë 7 Shkurt– 15 Maj 2014.

34 Çështja GJEDNJ -së Ramanauskas kundër Lituanisë, Aplikim nr. 74420/01, datë 05 shkurt 2008,pg.51.

35 Cështja GJEDNJ-së Ramanauskas kundër Lituanisë, Aplikimi nr.4420/01,(2008) pg,54; Vanyan kundër Rusisë, Aplikimi nr. 53203/99, (2005) pg .46; Teixeira de Castro kundër Portugalisë, Aplikimi nr. 25829/94, (1998) pg, 35-36.

36 Cështja GJEDNj-së Ramanauskas kundër Lituanisë, pg 54.

37 Shiko cështjen GJEDNj-së Sequeira kundër Portugalisë, Aplikimi nr. 73557/01, datë 06 Maj 2003, pg. 39.

38 Cështja GJEDNj-së Eurofinacom, Aplikimi 58753/00, datë 07 Shtator 2004.

39 Shiko cështjen GJEDNj-see Khudobin kundër Rusisë, Aplikimi nr.59696/00, datë 03 Mars 2005, pg.35; Cështja GJEDNj-*së* Ramanauskas kundër Lituanisë, pg. 60.

akuzohet dhe dënohet një person duhet ti paraqiten dhe të vlerësohen nga gjyqtari i çështjes.[40]

Në një vendim të fundit të Kolegjit Penal të Gjykatës së Lartë [41]është marrë në shqyrtim rasti i një individi të akuzuar për veprën penale "Ushtrimi i ndikimit të paligjshëm". Rezulton se në fazat e para ka pasur dyshime se një pedagog i një universiteti publik, merrte para në këmbin të notave të mira nga studentët e tij. Organi procedues, vendosi të autorizojë një person për kryerjen e veprimeve simuluese me personin që dyshohej se mblidhte shumat për llogari të subjektit të dyshuar. Pasi personi në fjalë mori shumat përkatëse nga agjenti i infiltruar u në arrestimi i tij. Këto veprime ishin shoqëruar edhe me përgjime ambientale dhe vëzhgime. Në vijim rezultoi se Gjykata e Shkallës së Parë e deklaroi të pafajshëm të akuzuarin pasi fakti nuk përbën vepër penale, ndërsa Gjykata e Apelit vendosi lënien në fuqi me arsyetimin se fakti nuk ekziston.

Ajo çka përbën me rëndësi në arsyetimin e Kolegjit Penal është analiza që i ka bërë fakteve nëse metoda speciale e hetimit "Veprimet simuluese", e përdorur nga akuza gjatë hetimit të kësaj çështje është marrë në kufijtë dhe sipas procedurës së përcaktuar në ligj, por edhe raporti që ekziston midis një veprimi simulues që fillon nga organi procedues I bazuar në disa indicje, prova dhe provokimi në vetvete për ta prodhuar faktin. Pra duhet patur parasysh që veprimtaria e organit procedues nuk duhet të jetë e tillë që të krijojë, nxisi, apo t'I bashkohet veprimeve të një individi privat. Roli I organit procedues nëpërmjet agjentit infiltrues duhet të jetë pasiv. Në lidhje me gjykatat që gjykojnë raste të kësaj natyre, sipas vendimit ë sipërcituar duhet patur kudjes edhe në citimin e praktikës së GJEDNJ-së si rasti *Ramanauskas kundër Lituanisë,* që merret si një vendim "pilot", pasi në rastin konkret bëhet dallimi I qartë mesa asaj që kosiderohet si provokim, nisje e një procedure simuluese pa autorizimin e organit proces, kryerjen e veprimeve me iniciativë të oficerit të policisë gjyqësore, dhe një procedure të rregullt që fillon mbi bazat një dyshimi të arsyeshëm dhe shoqërohet në të gjitha fazat e tij nga një vendimarrje e legjitimuar nga gjykata dhe vetë prokurori.

40 Ledi Bianku, Jurisprudenca e Gjykatës së Strazburgut(Edlora 2007) ,Çështja GJEDNJ-*së* Atlan kundër Mbretërisë së Bashkuar*;* Aplikim nr.36533/97,datë 19.06.2001, fq.344.

41 Me nr. Nr. 00 – 2022 – 362 i Vendimit (118) datë 14.04.2022.

KONKLUZIONE E REKOMANDIME

Krimi ekonomik një fenomen i cili nuk njeh kufi, hera herës shfaqet si bashkëshoqëruese e një sërë krimesh të organizuara si produkt i tyre apo i marrëdhënies që synohet të cenohet. Kompleksiteti shfaqet se veprimtari kriminale nuk është vetëm një kategori juridike e ndëshkueshme por ndërthur elemente social-ekonomike me ndikim të pashmangshëm të bazat e shtetit të së drejtës.

Një nga veprat penale me të rëndësishme për tu analizuar në kuadër të krimit ekonomik është padyshim korrupsioni, i cili në vetvete cenon shoqërinë dhe zhvillimin e saj në shumë dimensione. edhe se ka ekzistuar që me gjenezën e shoqërisë kjo nuk zbeh faktin se minon parime bazë si: barazia, paanësia, merita, integriteti dhe në tërësi gjithë themelet e shtetit të së drejtës.

Teknika të tilla hetimore tradicionale në kësisoj veprash kryesisht të konsideruara si "pa viktima" për të cilat dhe raportimet janë të ulëta, kanë treguar se nuk janë efektive. Në këtë këndvështrim hetimet penale kanë sjellë si domosdoshmëria përdorimin e një sërë teknikash speciale në zbulimin e tyre. Këto metoda janë veçanërisht invazive dhe tashme gjenden të parashikuar në legjislacionet e shumë vendeve ashtu dhe në nivel të aquis comunitare. Në Shqipëri rregullimi ligjor është relativisht i vonë, në ndryshimet e K. Pr. Penale të vitit 2004, dhe janë përdorur kryesisht në këto drejtime: për hetimin e veprave penale në fushën e narkotikëve, trafiqeve të paligjshme e krimit financiar e terrorizmit etj. Zbatimi në praktikë i këtyre teknikave shfaq problematike kryesisht në fushën e të drejtave të njeriut. Për sa më sipër njohja e tyre rrit efikasitetin dhe ul abuzivizmin.

Bibliografia

Doktrinë, botime, publikime, raporte

1. Barrocu Giovanni, "Le indagini sotto copertura ", Jovene editore, 2011.
2. Bianku Ledi, "Jurisprudenca e Gjykatës së Strazburgut" Edlora, 2007.
3. Block, Ludo "EU joint investigation teams:Political ambitions and police practices "London: Routledge,.2011.
4. Clive. Harfield, "Pro-activity, partnership and prevention: the UK contribution to policing organised crime in Europe. "The

Police Journal (vol. 73, nr.2, 2000).

5. Cutting P. D. “The technique of controlled delivery as a weapon in dealing ëith illicit traffic in narcotic drugs and psychotropic substances” Janar.1998,
6. Eliora Elezi “Teknikat speciale te hetimet. Veprimet simulese dhe agjenti infiltruar”. Temë e mbrojtur nën udheheqjen e A. Xholi Shkolla e Magjistraturës viti 2017.
7. Hay Bruce, “Sting Operations, Undercover Agents, and Entrapment”, Missouri Law Review,Vol.70, Nr.2 ,2005.
8. Islami Halim; Hoxha Artan, dhe Panda Ilir, ”Procedura Penale” Tiranë 2011.
9. Joh Elizabeth, “Breaking the law to enforce it.Undercover Police participation in crime” Stanford Law ReviewVol.62, Nr.1, Dhjetor, 2009, fq. 155-198.
10. Kruisbergen, Edwin W., De Jong Deborah and R. Kleemans Edward “Undercover Policing. Assumptions and Empirical Evidence” botuar në British Journal Criminology, 2011, Vol.51 nr. 2.
11. La Rue, Frank, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” aksesuar në adresën <www.ohchr.org> në datë 04 maj 2017.
12. Lauren, Hutton “Instrumenti 5, Mbikëqyrja e mbledhjes se informatave” Mbikëqyrja e Shërbimeve të Inteligjencës:Pako e Instrumenteve, 2012. Aksesuar në datë 20 Mars 2017 në adresën < www.dcaf.com>
13. Laurentiu, Giurea “Special methods and techniques for investigating drug trafficking” International Journal of Criminal Investigation Vol. 3,Nr. 2 / 2013 fq.137-146.
14. Mahney, Paul “Right to a fair trial in crimiminal matters, under article 6 E.C.H.R” National Judicial Conference Dublin,10-11 Nëntor 2001.
15. McDermott, Paul Anthony “Undercover Investigations Human Rights” 9-th Annual National Prosecutors Conference, 24 Maj 2008.
16. Sciacchitano, Giusto “Lufta kundër krimit të organizuar transnacional në hapësirën juridike dhe gjyqësore evropiane” Itali - Shqipëri: Instrumente ligjorë dhe teknika të luftës kundër

krimit të organizuar transnacional. “Përballje përvojash., UNICRI, 2007.

17. Sijerçiq – Çoliq, Hajrija, Haliloviq Haris, “E drejtë procedurës Penale në vështrim të posacëm në procedurën penale në Kosovë” përktheu nga kroatishtja: Mustafë Reçica ,Prishtinë, 2007

USE AND DEVELOPMENT OF TECHNOLOGY IN THE PREVENTION AND IDENTIFICATION OF THE CRIMINAL OFFENCES IN THE PUBLIC PROCUREMENT FIELD

Dr. Fjorida BALLAURI (KALLÇO)[1]

fjori.k@gmail.com

Msc. Josi BALLAURI[2]

josiballauri@gmail.com

Abstract

Since 2007, Albania has applied the e-procurement system, as an instrument in the fight against corruption in the field of public procurement. This system, above all, aimed to regulate and solve one of the biggest problems in the field of procurement in Albania: - lack of transparency, avoiding inequality in tenders of economic operators and preventing corruption. Despite the fact that e-procurement has influenced the prevention of abusive cases and illegal profits, the phenomenon continues to exist and corruption in the field of public procurement remains one of the biggest problems, not only in Albania. The procurement of goods and services from public funds is at risk of being harmed at any time by the private interests of officials, and therefore is provided as a legal relationship that is specifically protected by criminal law.

Albanian legislation has also given special importance to legal restrictions

1 Lecturer in the Faculty of Security and Investigation, Security Academy, Albania

2 Administrative Director, Directorate of Government Services, Albania

for conflict of interest in public procurement. This is due to the fact that the public property are at risk at any time to be harmed by the action of the private interests of the officials involved in this decision-making. The Law on Prevention of Conflict of Interest in Article 21, prohibits senior officials and persons related to them, to benefit directly or indirectly from contracts with a public institution, considering the conclusion of a contract as a particular public decision-making and at risk of being compromised by the private interests of officials.

This paper aims to make a modest analysis of the effectiveness of the electronic system that is currently in operation in the field of public procurement and the possibility of technological innovations through cross-checking of electronic data, in order to identify and prevent administrative violations and criminal offenses in the field of public procurement.

Keywords: *public procurement, electronic system, technology, official, restriction*

PËRDORIMI DHE ZHVILLIMI I TEKNOLOGJISË NË PARANDALIMIN DHE IDENTIFIKIMIN E VEPRAVE PENALE NË FUSHËN E PROKURIMIT PUBLIK.

Dr. Fjorida BALLAURI (KALLÇO)[3]

fjori.k@gmail.com

Msc. Josi BALLAURI[4]

josiballauri@gmail.com

Abstrakt

Një ndër instrumentat që vendi jonë ka aplikuar në luftën kundër korrupsionit në fushën e prokurimit publik është sistemi i prokurimit elektronik. Sistemi, mbi të gjitha ka synuar të rregullojë dhe zgjidhë një ndër problemet më të mëdha në fushën e prokurimeve në Shqipëri- mungesën e transparencës, shmangien e pabararazisë në tendera të operatorëve

3 LektornëFakultetin e SigurisëdheHetimi-Akademia e Sigurisë, Tiranë.

4 DrejtorAdministrativ-Drejtoria e ShërbimeveQeveritare, Tiranë.

ekonomikë dhe parandalimin e korrupsionit. Pavarësisht faktit se prokurimi elektronik ka ndikuar në parandalimin e rasteve abuzive dhe përfitimeve të paligjshme, fenomeni vazhdon të ekzistojë dhe korrupsioni në fushën e prokurimeve publike mbetet nje nga problemet më të mëdhaja, jo vetëm të vendit tonë. Fusha e prokurimit të mallrave dhe shërbimeve nga fondet publike është e rrezikuar në çdo kohë të dëmtohet nga interesat private të zyrtarëve, prandaj dhe është parashikuar si një marrëdhënie juridike që mbrohet posaçërisht nga ligji penal.

Legjislacioni jonë gjithashtu i ka dhënë një rëndësi të veçantë kufizimeve ligjore dhe trajtimit të rasteve të konfliktit të interesave në prokurimet publike. Kjo për vet faktin se nisur nga rëndësia dhe vlerat pasurore publike që kanë, janë të rrezikuara në çdo kohë që të dëmtohen nga veprimi i interesave private të zyrtarëve të përfshirë në këtë vendimmarrje. Ligji për parandalimin e konfliktit të interesave në nenin 21, ndalon në mënyrë absolute qëzyrtarëtë lartë dhe persona të lidhur me ta, tëpërfitojnë drejtpërdrejtë ose në mënyrë të tërthortënga kontratat me palë një institucion publik, duke e konsideruar lidhjen e një kontrate si një vendimmarrje të veçantë publike dhe me risk për t'u dëmtuar apo cënuar nga interesat private të zyrtarëve.

Ky punim synon të bëjë një analizë modeste të efektivitetit të sistemit elektronik që sot është në funksion në fushën e prokurimit publik dhe mundësinë e risive teknologjike nëpërmjet kryqëzimit të të dhënave elektronike, më qëllim identifikimin dhe parandalimin e shkeljeve administrative apo veprave penale në fushën e prokurimit publik.

Fjalëkyçe: *prokurim publik, sistem elektronik, teknologji, zyrtar, ndalim.*

1.Hyrje

Fusha e prokurimit publik, ankandeve dhe koncensioneve për fonde dhe pasuri publike,mbetenedhe sot të ndjeshme nga rreziku për korrupsion dhe konflikt interesi. Kontratat për prokurime publike, për shkak të rëndësisë dhe vlerave pasurore publike që kanë, janë të rrezikuara në çdo kohë që të dëmtohen nga veprimi i interesave private të zyrtarëve të përfshirë në këtë vendimmarrje, apo në funksione publike të tilla që mund të lehtësojnë përfitime të padrejta për vetë ose persona të tretë.

Me qëllim parandalimin e rasteve të abuzimit me prokurimet publike, ligjvënësi ka parashikuar disa instrumente ligjorë dhe konkretisht: Ligji 162/2020 "Për prokurimin publik", ka parashikuar se autoriteti kontraktor është i detyruar të refuzojë një ofertë ose kërkesë për pjesëmarrje në tender,

nëse operatori ekonomik ose kandidati është në kushtet e konfliktit të interesit. (neni 19).

Nga ana tjetër, ligji nr.9367, datë 7.4.2005 *"Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike"* i ndryshuar (ligji PKI), i ka kushtuar një nen të veçantë ndalimit të lidhjes së kontratave me palë një institucion publik(neni 21), duke e konsideruar lidhjen e një kontrate si një vendimmarrje të veçantë publike dhe me risk për t'u dëmtuar apo cënuar nga interesat private të zyrtarëve.

Neni 21 i ligjit për parandalimin e konfliktit të interesave ka sanksionuar ndalimet e interesave private të zyrtarëve në dy nivele të ndryshme. Janë parashikuar ndalime të posaçme për kategori të caktuara zyrtarësh, pavarësisht rolit të tyre në lidhjen e kontratave me palë një institucion publik (pikat 1 dhe 2 të nenit 21 të ligjit) dhe ndalime të tjera që varen nga roli konkret i zyrtarit në vendimmarrjen për këto kontrata (pika 3 e nenit 21 të ligjit).

Rreziku për përfitime të padrejta të zyrtarëve nga kontratat publike, fonde apo pasuri shtetërore, potencialisht ekziston për shkak të funksionit dhe pozicionit të tyre, duke përdorur "ndërhyrjet" në kompetencat e zyrtarëve vartës. Për këtë arsye, duke synuar parandalimin e abuzimit për shkak të pozicionit publik, ligji ka parashikuar disa ndalime të posaçme të sanksionuar në nenin 21 të ligjit PKI sipas së cilës, zyrtarë të lartë të shtetit nuk mund të përfitojnë nga kontratat me palë një institucion publik, pavarësisht se ata mund të mos jenë në asnjë moment të përfshirë apo pjesë e vendimmarrjes për lidhjen e asaj kontrate. Pra, kufizimi i përfitimit nga fondet apo pasuria publike, në këtë rast, është i lidhur vetëm me pozicionin e zyrtarit dhe jo me vendimmarrjen konkrete apo rolin e zyrtarit në këtë vendimmarrje.

Në ligj është përcaktuar shprehimisht se cili do të jetë rrethi i zyrtarëve të cilëve ju ndalohet në mënyrë absolute të përfitojnë nga kontratat me palë një institucion publik. Konkretisht në pikën 1 të nenit 21 të ligjit të parandalimit të konfliktit të interesave është përcaktuar se:

"*1. Asnjë individ, kur ky njësohet me një zyrtar në njërin nga funksionet e përcaktuara në kreun III, seksioni 2 të këtij ligji, gjyqtarët e prokurorët në nivelin e gjykatës së shkallës së parë e në atë të apelit, dhe asnjë shoqëri tregtare, ortakëri a shoqëri e thjeshtë, ku ky zyrtar zotëron, në mënyrë aktive apo pasive, aksione a pjesë në kapital, në çfarëdo sasie, nuk mund të lidhë kontratë ose nënkontratë me asnjë institucion publik.*

Për zyrtarët e nivelit të mesëm drejtues të parashikuar ne nenin 31 dhe

për zyrtarët e parashikuar në nenin 32 të kreut të III, seksioni 2 të këtij ligji, ndalimi sipas pikës 1 të këtij neni, për shkak të interesave private të zyrtarit, të përcaktuara në këtë pikë zbatohet vetëm në lidhjen e kontratave në fushën e territorit dhe të juridiksionit të institucionit, ku punon zyrtari. Ky ndalim zbatohet edhe kur palë është një institucion i varësisë".

Ndalimet e përcaktuara në nenin 21 pika 1 të ligjit nr.9367, datë 7.4.2005, i ndryshuar, (duke mbajtur parasysh në çdo rast përjashtimet që vet ligji ka përcaktuar në rastet e ndalimit të lidhjes së kontratave), zbatohen, në të njëjtën masë, edhe për personat e lidhur[5] me zyrtarët e lartpërmendur sipas nenit 24 të tij. Sipas konceptit të ligjit të parandalimit të konflikti të interesit, rrethi i personave të lidhur me zyrtarin janë bashkëshorti/ja, bashkëjetuesi/ja, fëmijët madhorë dhe prindërit e zyrtarit dhe bashkëshortit/es.

Me ndryshimet e ligjit të parandalimit të konfliktit të interesave miratuar me ligjin nr.86/2012 datë 18.9.2012, zyrtarit apo personave të lidhur me të i ndalohet tashmë edhe përfitimi nga kontratat publike me anë të nënkontraktimit. Me sanksionimin shprehimisht në ligj të këtij ndalimi, parandalohen rastet e gjetjes së klauzolave të mundshme për shmangien nga kufizimet ligjore, duke hequr kështu mundësitë e pjesëmarrjeve fiktive në tendera publikë apo kontrata administrative, të cilat efektivisht realizoheshin nëpërmjet nënkontraktimit, nga ata persona/shoqëri tregtare, që për shkak të kufizimeve ligjore nuk mund të përfitojnë nga fondet apo pasuria publike.

Ndërkohë në pikën ç) të nenit 99 i ligjit 162/2020 "Për prokurimin publik", parashikohet se:

"Për çdo kontratë ose marrëveshje kuadër që mbulohet nga ky ligj dhe sa herë që krijohet një sistem dinamik blerjeje, autoriteti ose enti kontraktor harton një raport me shkrim, që përfshin të paktën sa më poshtë:

a) emrin dhe adresën e autoritetit ose enti kontraktor, objektin dhe vlerën e përllogaritur të kontratës, të marrëveshjes kuadër ose sistemit dinamik të blerjes sipas rastit;

b) rezultatet e përzgjedhjes së kandidatëve, ofertuesve dhe/ose uljes së numrit të tyre, sipas parashikimeve në këtë ligj, përkatësisht: i. emrat e kandidatëve ose ofertuesve të përzgjedhur dhe arsyet për përzgjedhjen e tyre; ii. emrat e kandidatëve ose ofertuesve të refuzuar dhe arsyet për refuzimin e tyre;

5 Neni 24, pika 1 e ligjit nr.9367, datë 7.4.2005, i ndryshuarparashikon se: "*Rrethi i personavetëlidhur me zyrtarin, nëzbatimtëndalimevetëpërcaktuaranënenin 21 dhenënenin 22 tëkëtijligji, përbëhetngabashkëshorti/ja, bashkëjetuesi/jafëmijëtnëmoshëmadhoredheprindërit e zyrtarit e tëbashkëshortit/esdhebashkëjetuesit/es".*

c) arsyet për refuzimin e ofertave anomalisht të ulëta;

ç) emrin e ofertuesit të suksesshëm dhe arsyet pse është zgjedhur oferta e tij dhe, kur dihet, ***përqindjen e kontratës ose marrëveshjes kuadër që ofertuesi i suksesshëm planifikon të nënkontraktojë te palë të treta, emrat e nënkontraktorëve të kontraktorit kryesor, nëse ka;***

Sipas parashikimit të kësaj dispozite, rezulton se përzgjedhja e subjektit nënkontraktor varet nga propozimi i operatorit ekonomik, duke mos ju nënshtruar ndonjë procedure kualifikimi apo konkurrimi dhe aktualisht nuk ka instrumente kontrollues që vihen në lëvizje për këtë qëllim. Ndryshe nga praktika për operatorët ekonomikë, të cilët plotësojnë detyrimisht "Deklaratën mbi konfliktin e interesit"si pjesë e dokumenteve standarde të prokurimit.

Përfshirja në nenin 21 të ligjit PKI edhe nënkontraktimet, detyron institucionet përgjegjëse të krijojnë instrumentat që do të identifikojnë dhe kontrollojnë kompanitë që do të përfshihen si nënkontaktore në një kontratë për shërbime mallra etj., të prokuruara nga fondet publike[6]. Dokumenti"Deklarata e konfliktit të interesave", duhet të plotësohet me ndryshimet e fundit ligjore dhe operatorët ekonomikë nëpërmjet përfaqësuesve ligjore, duhet të deklarojnë nën përgjegjësinë e tyre se, asnjë nga zyrtarët përcaktuar në Kreun III, Seksioni II te ligjit nr. 9367, datë 7.4.2005, nuk zotëron interesa private në mënyrë të drejtpërdrejtë ose të tërthortë me kompaninë që ai përfaqëson apo me kompaninë nënkontraktore të tij.

2. Disa instrumenta ligjorë për parandalimin e veprave penale në fushën e prokurimit publik

Me qëllim parandalimin e rasteve të abuzimit me prokurimet publike, ligjvënësi ka parashikuar disa instrumente ligjorë dhe konkretisht:

- Ligji 162/2020 "Për prokurimin publik", ku ka parashikuar se autoriteti kontraktor është i detyruar të refuzojë një ofertë ose kërkesë për pjesëmarrje në tender, nëse operatori ekonomik ose kandidati është në kushtet e konfliktit të interesit (neni 19).
- Ligji nr.9367, datë 7.4.2005 "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike" i ndryshuar, i ka kushtuar një nen të veçantë ndalimit të lidhjes së kontratave me palë një institucion

6 F.Ballauri, "Konflikti i interestitdhevepratpenalenwfushwn e prokurimevepublike", Jus&Justicia, Nr.9, 2015.

publik (neni 21), duke e konsideruar lidhjen e një kontrate si një vendimmarrje të veçantë publike dhe me risk për t'u dëmtuar apo cenuar nga interesat private të zyrtarëve.

- Neni 21 i ligjit për parandalimin e konfliktit të interesave ka sanksionuar ndalimet e
- interesave private të zyrtarëve në dy nivele të ndryshme:
- ndalime të posaçme për kategori të caktuara zyrtarësh, pavarësisht rolit të tyre në lidhjen e kontratave me palë një institucion publik (pikat 1 dhe 2 të nenit 21),
- ndalime të tjera që varen nga roli konkret i zyrtarit në vendimmarrjen për këto kontrata (pika 3 e nenit 21 te ketij ligji).
- Neni 258 i Kodit Penal të Republikës së Shqipërisë, ku ka parashikuar se:

"Shkelja e barazisësëpjesëmarrësvenëtenderaoseankandepublike.

"Kryerja nga personi i ngarkuar në funksione shtetërore apo në shërbim publik i veprimeve në kundërshtim me ligjet që rregullojnë, lirinë e pjesëmarrjes dhe barazinë eshte ta sve në tendera ose ankande publike, për të krijuarav antazhe ose privilegje të padrejta për të tretet, dënohet me burgim gjer në tre vjet".

Risku për përfitime të padrejta të zyrtarëve nga kontratat publike, fonde apo pasuri shtetërore, ekziston për shkak të funksionit dhe pozicionit të tyre, nisur nga rreziku për të përdorur "ndërhyrjet" në kompetencat e zyrtarëve vartës.

Për këtë arsye, duke synuar parandalimin e abuzimit për shkak të pozicionit publik, ligji ka parashikuar disa ndalime të posaçme të sanksionuar në nenin 21 të ligjit PKI sipas së cilës:

Zyrtarë të lartë të shtetit nuk mund të përfitojnë nga kontratat me palë një institucion publik, pavarësisht se ata mund të mos jenë në asnjë moment të përfshirë apo pjesë e vendimmarrjes për lidhjen e asaj kontrate.Pra, kufizimi i përfitimit nga fondet apo pasuria publike, është i lidhur vetëm mefunksionin publik të zyrtarit dhe nuk ka lidhje me vendimmarrjen konkrete apo rolin e zyrtarit në këtë vendimmarrje.

Subjekte të veprës penale mund të jenë të gjithë kategoritë e zyrtarëve që përfshihen në procedurat e vendimmarrjes së prokurimeve ose ankandeve publike, që nga përcaktimi i termave të referencës, fondit limit e deri ne lidhjen dhe ekzekutimin e kontratës. Këta zyrtarë me qëllim që të krijojnë

avantazhe për subjekte të caktuara mund të krijojnë lehtësira që mundësojnë shpalljen fitues të një operatori ekonomik, në këmbim të përfitimeve që ky i fundit premton apo i jepzyrtarit. Kjo mund të realizohet nëpërmjet votimit në komisionin e vlerësimit të ofertave të zyrtarit përkatës, përcaktimit të kritereve që favorizojnë një operator të caktuar, përcaktimin e kritereve vlerësuese evazive, etj.

Nga ana subjektive[7], krimi kryhet me dashje të drejtpërdrejtë dhe me qëllim për të krijuar avantazhe ose privilegje të padrejta për të tretët, nisur nga motivet se e ka të afërm, mik, shok apo ka interesa të tjerë materiale apo morale. Pra, ato interesa private të renditura në mënyrë shteruese edhe në ligjin e konfliktit të interesave, për shkak të sëcilave zyrtari duhet në çdo rast të shmanget nga vendimmarrja. Ekzistenca e konfliktit të interesave në vendim marrje të tilla, vëpër ballë përgjegjësisë institucionin përkatës apo institucionin e pror për të kontrolluar më tej procedurat e ndjekura dhe vlerësimin nëse zyrtari/rët kanë konsumuar elementët e ndonjë veprepenale duke vepruar me keq besim për të ardhur pasoja konkrete. Nga ana tjetër, duhet theksuar se vepra penale e shkeljes së barazisë në tendera dhe ankande konkurron edhe me veprën penale të korrupsionit pasiv të zyrtarëve publikë (neni 259 dhe 260 i Kodit Penal) përderisa interesi privati marrjes së përfitimit të parregullt për vetë apo për të tjerë, lidhet me kryerjen apo mos kryerjen e një veprimi që lidhet me funksionin e tij.

3. Kategoritë e zyrtarëve të cilëve iu ndalohet të përfitojnë nga prokurimet publike

Referuar nenit 21 pika 1 e ligjit nr. 9367, datë 7.4.2005 *"Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike"* i ndryshuar kategoritë e zyrtarëve të përfshirë në ndalimin e nenit 21 pika 1 janë:

- Presidenti i Republikës;
- Kryeministri, Zëvendëskryeministri, Ministrat, Zëvendësministrat;
- Deputetët;
- Kryetari i Kontrollit të Lartë të Shtetit (KLSH);
- Avokati i Popullit;
- Anëtarët e Komisionit Qendror të Zgjedhjeve;
- Inspektori i Përgjithshëm i Inspektoratit të Lartë të Deklarimit dhe të Kontrollit të Pasurive;

7 IsmetElezi, "E drejtaPenale, pjesa e posaçme" Tiranë2018, f.425.

- Anëtarët e enteve rregullatore (Këshilli Mbikëqyrës i Bankës së Shqipërisë, përfshirë Guvernatorin dhe Zëvendësguvernatorin, të konkurrencës, telekomunikacionit; energjisë; furnizimit me ujë, të sigurimeve, letrave me vlerë, mediave;
- Gjyqtarët e Gjykatës Kushtetuese, Gjyqtarët e Gjykatës së Lartë; anëtarët e Këshillit të Lartë Gjyqësor, Prokurori i Përgjithshëm;
- Gjyqtarët e prokurorët në nivelin e gjykatës së shkallës së parë e në atë të apelit.
- Zyrtarët e nivelit të lartë drejtues sipas legjislacionit të shërbimit civil: Sekretarët e Përgjithshëm, drejtorët e departamenteve, drejtorët e përgjithshëm dhe pozicione të barazvlefshme me to;
- Nëpunësit e nivelit të mesëm drejtues, por vetëm për kontratat e lidhura në fushën e territorit dhe të juridiksionit të tyre;

Ndalimet e përcaktuara në nenin 21 pika 1 të ligjit nr.9367, datë 7.4.2005, i ndryshuar, sipas konceptit të ligjit të parandalimit të konflikti të interesit (neni 24 i ligjit PKI), përfshijnë dhe rrethin e personave të lidhur me zyrtarin që janë bashkëshorti/ja, bashkëjetuesi/ja, fëmijët madhorë dhe prindërit e zyrtarit dhe bashkëshortit/es.

Ligji përcakton shprehimisht se, jo vetëm zotërimi i interesave të drejtpërdrejtë, por edhe të tërthortë nga ana e zyrtarit ose personave të lidhur me të, përbëjnë interes privat të zyrtarit. Pra, konsiderohet interes privat i zyrtarit ose personave të lidhur me të, edhe nëse ai/ata zotëron/jnë aksione, pjesë në kapital, etj., në një shoqëri që nga ana e vet zotëron aksione apo pjesë në kapital në një shoqëri të dytë, ku kjo e dyta është palë në kontratë (neni 25 pika 2 e ligjit nr.9367, datë 7.4.2005 i ndryshuar).Gjithashtu, objekt i ndalimit të ligjit të parandalimit të konfliktit të interesave është edhe nënkontraktimi.

Personat e lidhur me zyrtarin, në kuptim dhe zbatim të ligjit të parandalimit të konfliktit të interesave janë bashkëshorti/ja, fëmijët në moshë madhore dhe prindërit e zyrtarit dhe bashkëshortit/es". Ligji përcakton shprehimisht se, jo vetëm zotërimi i interesave të drejtpërdrejtë, por edhe të tërthortënga ana e zyrtarit ose personave të lidhur me të, përbëjnë interes privat të zyrtarit. Pra, konsiderohet interes privat i zyrtarit ose personave të lidhur me të, edhe nëse ai/ata zotëron/jnë aksione, pjesë në kapital, etj., në një shoqëri që nga ana e vet zotëron aksione apo pjesë në kapital në një shoqëri të dytë, ku kjo e dyta është palë në kontratë (neni 25 pika 2 e ligjit nr.9367, datë 7.4.2005 i ndryshuar).

Në nenin 19, pika 2 dhe 3 e ligjit nr.162/2020 "Për prokurimin publik",

parashikohet se:

"2. Autoriteti ose enti kontraktor refuzon një ofertë ose një kërkesë për pjesëmarrje në tender nëse:

a) kandidati ose ofertuesi i jep ose premton t'i japë, drejtpërdrejt ose tërthorazi, një zyrtari apo punonjësi një shpërblim në çfarëdolloj forme, mundësi punësimi ose mall, shërbim ose vlerë, si stimul për një akt, vendim ose procedurë që ndërmerr autoriteti ose enti kontraktor për procedurat e prokurimit;

b) kandidati ose ofertuesi është në kushtet e konfliktit të interesit sipas parashikimeve të legjislacionit në fuqi për parandalimin e konfliktit të interesave;

c) kandidati ose ofertuesi në të njëjtën procedurë janë në rrethin e personave të lidhur sipas legjislacionit për parandalimin e konfliktit të interesave.

Refuzimi dhe arsyet për një veprim të tillë duhet të dokumentohen dhe i komunikohen menjëherë dhe zyrtarisht kandidatit ose ofertuesit në fjalë.

3. Vendimet e marra nga autoriteti ose enti kontraktor në përputhje me pikën 2 të këtij neni, nuk pengojnë kallëzimin penal në organet përkatëse, kur aktet apo veprimet në fjalë përbëjnë vepër penale".

Referuar vendimeve dhe udhëzimeve të Agjencisë së Prokurimit Publik në dokumentet Standarde të Prokurimeve, tashmë është përfshirë në të gjitha rastet edhe "*Deklarata mbi konfliktin e interesit*", dokument i detyrueshëm për plotësim nga operatorët ekonomikë. Ky është një dokument i detyrueshëm për plotësim, mungesa e të cilit çon automatikisht në skualifikim të kompanisë që kërkon të konkurrojë për fonde publike.

Sipas këtij dokumenti, operatori ekonomik nëpërmjet përfaqësuesit të tij ligjor, deklaron nën përgjegjësinë e tij se është në dijeni të ndalimeve dhe kufizimeve të ligjit të parandalimit të konfliktit të interesave dhe se asnjë nga zyrtarët përcaktuar në Kreun III, Seksioni II te ligjit nr. 9367, datë 7.4.2005, dhe në këtë deklaratë, nuk zotëron interesa private në mënyrë të drejtpërdrejtë ose të tërthortë me personin juridik që ai përfaqëson.

"*Deklarata mbi konfliktin e interesit*" , është një dokument vetdeklarimi, vërtetësia e të cilit nuk rezulton t'i nënshtrohet ndonjë kontrolli institucional të autoritetit kontraktor ose ndonjë institucioni tjetër shtetëror.

Pyetja që shtrohet këtu është:

Si mund ta identifikojë autoriteti kontraktor, operatorin ekonomik që duhet të skualifikohet për shkak të ndalimit të nenit 21 të ligjit PKI?

Konstatojmë se ky ndalim ligjor, i parashikuar nga neni 21 i ligjit PKI, nuk kontrollohet nga autoritetet kontraktore, por as nga ndonjë instrument tjetër ligjor të institucioneve të tjera si ILDKPKI, APP, KPP, KLSH.

4. Disa konstatime dhe problematika në lidhje me fushën e prokurimeve publike dhe konfliktit të interesave

Së pari, në nenin 40, pika 2 e ligjit nr.ligjit nr.9367, datë 7.4.2005 i ndryshuar parashikohet se:

"1. Aktet dhe kontratat administrative të çdo institucioni publik dhe ankimimi ndaj tyre, të nxjerra në kushtet e konfliktit faktik ose në dukje të interesave, janë të pavlefshme, sipas kuptimit të këtij termi dhe parimeve e procedurave të përcaktuara në Kodin e Procedurave Administrative.

2. Çdo kontratë civile, e lidhur në kundërshtim me pikat 1, 2, 3 e 6 të nenit 21 dhe pikën 3 të nenit 24 të këtij ligji, ose në çdo rast tjetër, kur ajo është lidhur në praninë e konfliktit faktik ose në dukje të interesit, nuk krijon asnjë pasojë juridike".

Pra, kontrata për një prokurim publik, e ndërmarrë në kushtet e ndalimit të nenit 21 të ligjit PKI, është absolutisht e pavlefshme, parashikuar shprehimisht në nenin 40, pika 2 e ligjit PKI.Gjithashtu, ndalimi përfshin dhe rastet e nënkontraktimit.

Së dyti, shkelja e ligjit nga ana e Komisionit të Vlerësimit të Ofertave, duke mos verifikuar me dashje, nga neglizhenca, ose nga pamundësia këtë ndalim ligjor, duke lënë mundësinë e përfitimit të padrejtë të operatorëve ekonomikë që i ndalohet me ligj të konkurojnë për fonde publike, cënon haptazi barazinë e pjesëmarrësve në tendera apo ankande publike (duke plotësuar elementët e veprës penale të parashikuar në nenin 258 të Kodi Penal).

Së treti, konstatojmë se nëse këto raste nuk parandalohen në kohë (gjatë procedurave të prokurimit), mundësia e zbulimit gjatë kohës së ekzekutimit të kontratës apo dhe më vonë, bëhet gati e pamundur, sepse mungojnë instrumentat kontrollues për këtë element.

Së katërti, referuar raporteve[8] dhe statistikave të APP, KPP, KLSH,

8 Shikopërmëshumëraportetvjetoretë APP, KPP, ILDKPKI, KLSH përperiudhën 2012-2021

ILDKPKI, rezulton se monitorimi dhe kontrolli i zbatimit të ndalimeve të nenit 21 të ligjit PKI, është jashtë objektit të kontrollit të tyre. Praktikisht, askush nuk e kontrollon zbatimin e ndalimit të nenit 21 të ligjit të parandalimit të konfliktit të interesave.

Së pesti, konstatojmë se, Komisioni i Vlerësimit të Ofertave, praktikisht e ka të pamundur të identifikojë rastet e ndalimit absolut, për sa kohë që ata nuk e disponojnë listën (e përditësuar) të zyrtarëve deklarues në ILDKP dhe personave të lidhur me ta, të cilëve iu ndalohet të përfitojnë nga fondet apo pasuria publike.

Së gjashti, me hyrjen në fuqi të ligjit nr.6/ 2022 "Për regjistrin e pronarëve përfitues" të ndryshuar, lehtësohet mundësia e marrjes dhe shkëmbimit të të dhënave identifikuese të pronarëve/aksionerëve të operatorëve ekonomikë që operojnë në vendin tonë. Në këtë mënyrë kemi dy sisteme, njëri me regjistrin e zyrtarëve dhe personave të lidhur me ta, që sigurohet nga ILDKPKI dhe një sistem me regjsitrin e pronarëve/aksionerëve të operatorëve ekonomikë që operojnë në vendin tonë, sisteme këto që lehtësisht mund të ndërthurren për të identifikuar ato operatorë ekonomikë, të cilët e kanë të ndaluar me ligjin e konfliktit të interesave të përfitojnë nga fondet publike.

Nevoja e ngritjes së një sistemi elektronik për kontrollin e konfliktit të interesave në prokurime

nëfaqetzyrtaretëtyre.

5. Konkluzione dhe rekomandime

Nisur nga:

1. Numri i madh i operatorëve ekonomikë që operojnë dhe konkurojnë për fonde publike dhe pamundësia nga ana teknike e kontrolleve manuale në sistemin e QKB;
2. Fakti që lista e subjekteve deklarues ndryshon vazhdimisht, për shkak të ndryshimit të pozicionit të tyre të punës, apo dhe listës së personave të lidhur me ta;
3. Nevoja e luftës kundër korrupsionit dhe shpërdorimit të detyrës, me qëllim përfitimet e padrejta nga fondet dhe prokurimet publike;

Nevojitet ngritja e një sistemi elektronik për kontrollin e kufizimeve ligjore për shkak të konfliktit të interesave.

Me hyrjen në fuqi të ligjit nr.6/ 2022 "Për regjistrin e pronarëve përfitues" të ndryshuar, lehtësohet mundësia e marrjes dhe shkëmbimit të të dhënave identifikuese të pronarëve/aksionerëve të operatorëve ekonomikë që operojnë në vendin tonë.

Në vlerësimin tonë, ky sistem duhet të administrohet nga Agjencia e Prokurimit Publik, të jetë pjesë përbërëse e Sistemit Elektronik të Prokurimit dhe të përditësohet me të dhëna nga ILDKPKI, Drejtoria e Pergjithshme e Tatimeve dhe QKB, me qëllimin identifikimin në kohë të operatorëve ekonomikë, që për shkak të ligjit nuk mund të konkurojnë për fonde publike.

Përdorimi i teknologjisë në këtë rast, duke kryqëzuar të dhënat ekzistuese të sistemeve të ILDKPKI, Drejtorisë së Pergjithshme të Tatimeve dhe QKB, do të parandalonin shkeljet dhe disa forma të abuzimit me detyrën të zyrtarëve të lartë publikë në fushën e prokurimeve.

Bibliografia:

1. Kushtetuta e Republikës së Shqipërisë.
2. Kodi i Procedurave Administrative.
3. Kodi Penal i Republikës së Shqipërisë.
4. Ligj nr.9367, datë 7.4.2005,"Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike" , i ndryshuar.

5. Ligjinr.162/2020 “Për prokurimin publik”.
6. Ligji nr.6/ 2022 “Për regjistrin e pronarëve përfitues” të ndryshuar.
7. Ismet Elezi, “E drejta penale, Pjesa e posaçme”, Tiranë 2018.

Raportet vjetore të ILDKPKI 2012-2021, www.ildkpki.gov.al

Analizatv jetore të Agjencisë së Prokurimit Publik 2012-2021, www.app.gov.al

Raporte vjetore të Performancës 2012-2021 të KLSH, www.klsh.gov.al

"HIGH-TECH CRIMES AND CHALLENGES FOR THEIR INVESTIGATIONS."

MSC. INGRIDA BEHRI MUSTAFA[1]
studioligjorebehri@gmail.com

Abstract

Today's human population got dependable on cyber technologies bringing us a lot of benefits as well as nightmares. Some studies suggest that there are several billions internet connections worldwide and they are not only in hands of the Legal Forces, but rather with the criminals, terrorists and the other harmful actors. So, as we all are dependable on new technologies – our opponents are at the same position as well.

The development of crime through technology has brought on the other hand many challenges for the bodies and the policy of investigations and criminal and police prosecution.

Police organizations delineate boundaries and jurisdiction within which they operate and each command knows, with high degree of accuracy, the stretch and reach of its powers and tries to work within its bounds. However, this dynamics has been dramatically altered with the growth of digital technology and the corresponding emergence of technology-enabled crimes across nations' borders.

1 *Msc. INGRIDA BEHRI MUSTAFA was born in April 6, 1992. Graduated in Msc. International Public Law, at Faculty of Political and Legal Sciences, at Aleksander Moisiu University of Durres, in 2015. She has started her professional carrier as a notary assistant at a Public Notary and as a lecturer of European Law, and other law subjects at Faculty of Political and Legal Sciences, at Aleksander Moisiu University of Durres. She currently works as a lawyer in her Law Firm and studies Executive Master in Crimi*

Through this research article, we will talk about the challenges of the organized crime tomodern societies, their impacts to world's population, culture and economy and finally provide some correlations between the cyberspace and the criminal environment suggesting how some heavy cases in criminology could get investigated using computers, web and mobile technologies also we will examines the changing dynamics of high technology crime and how this development has challenged traditional policing policies and practices.

Key words: *cyber security, criminology, intelligence, high-tech crime, digital technology.*

Hyrje

Krimet e teknologjisë së lartë janë duke u shfaqur shumë shpejt në epokën dixhitale, me implikime të gjera për strategjitë tradicionale të policies dhe organeve të ndjekjes penale.Sfida e krimeve të teknologjisë së lartë ka kërkuar risi në politikat dhe praktikat e policisë në mbarë botën. Risi të tilla duhet të demonstrojnë një vlerësim të dinamikës së kufijve në epokën dixhitale dhe se si ajo ndikon në shtrirjen dhe modelet e krimit.Dy dekadat e fundit janë shënuar nga një ndryshim masiv në mënyrën se si qeniet njerëzore përdorin teknologjinë kompjuterike[2].Ndoshta, "*vrasësit, abuzuesit seksualë, shantazhuesit, hajdutët, spiunët dhe shumë kriminelë të tjerë kanë përdorur internetin për të lehtësuar krimet e tyre.Interneti u jep kriminelëve akses më të madh te viktimat, duke e zgjeruar shtrirjen e tyre nga një zonë e kufizuar gjeografike tek viktimat në mbarë botën*".[3]Hapësira kibernetike është e ndërlidhur me hapësirën fizike dhe si e tillë, siguria në hapësirën kibernetike është e nevojshme për një shoqëri me lundrim të qetë.[4] Është argumentuar se: "ajo që nevojitet është një konceptim i policimit në epokën e informacionit, një epokë në të cilën kufijtë kombëtarë janë më pak të shënuar dhe të qartë, ku informacioni është një mall dhe shqetësimet e

2 Holt, T.J. and Bossler, A.M. (2014).An assessment of the current state of cyber crime scholarship. Deviant Behaviour, 35: 1, 20-40. DOI: 10.1080/01639625. 2013.822209 Internet Crime Report (2015). Retreived October 2, 2016 from https://pdf.ic3.gov/2015_IC3Report.pdf

3 Casey, E. (2002). Cyberpatterns: Criminal behaviour on the internet. In B.Turvey (Ed.). Criminal Profiling: An Introduction to behavioral evidence analysis. Amsterdam: Elsevier Academic Press.

4 Leukfeldt, R., Veenstra, S. and Stol, W. (2013). High volume cybercrime and the organization of the police: The result of two empirical studies in Netherlands. International Journal of Cyber Criminology, 7 (1), 1 – 17.

fshehtësisë dhe sigurisë gjenden në një pjesë të madhe, në transnacionale. rrjeti i informacionit".[5]Parashikohet që, me rritjen e krimit kibernetik, bashkëpunimi policor përtej kufijve kombëtarë do të përmirësohet; por aktualisht, kriminelët kibernetikë mund të shfrytëzojnë shumë zbrazëtira.[6] Në thelb, "*ndërsa kriminalizimi i kalon gjithnjë e më shumë kufijtë shtetërorë apo edhe i injoron ata, ky mjedis social për të dhënë legjitimitet kulturor duhet të bëhet vetë transnacional*".[7]

Për të pasur një trajtim më të qartë dhe të të plotë të artikullit, le të ndalemi në trajtimin e disa termave konceptual të artikullit:

Krimet e teknologjisë së lartë

Krimi i teknologjisë së lartë është një term që përdoret për të përshkruar krimet që kryhen nëpërmjet teknologjisë së re elektronike dhe dixhitale të bazuar si interneti ose kompjuteri.Ato quhen gjithashtu krime kibernetike, krime kompjuterike dhe krime teknologjike, bazuar në fushën e ekzekutimit. Objektivi kryesor i krimit të teknologjisë së lartë është shkelja e privatësisë dhe vjedhja e të dhënave.[8]

Kriminelët mund të përdorin teknologjinë për të kryer krimet e mëposhtme: hakerim, frik, thyerje të fjalëkalimit, shkelje të së drejtës së autorit, phishing, vjedhje identiteti, farming, përhapje të kodeve me qëllim të keq, pornografi për fëmijë ndër të tjera. Karakteristikë e zakonshme e krimeve të teknologjisë së lartë është shfrytëzimi i boshllëqeve të bazuara në kompjuter/internet në kryerjen e aktiviteteve të paligjshme.Gjithashtu, për shkak se krimet e teknologjisë së lartë janë të bazuara në dixhital, ato nuk zbulohen lehtë.

Policimi pa kufi

Policimi pa kufi është përkufizuar si "çdo nga përpjekjet e ndryshme të

5 Jones, R. (2009). Cybercrime and internet security: A criminological introduction. In L. Edwards and C. Waelde.Law and the internet (pp. 601-621). Oxford: Hart Publishing.

6 Giddens, A. and Sutton, P.W. (2013).Sociology.(7 Ed.). Hoboken, NJ:John Wiley & Sons, Inc.

7 Cotterrell, R. (2015). The concept of crime and transnational networks of community. In V. Mitsilegas, P. Alldridge and L. Chelitotis (Eds.), Globalization, criminal law and criminal justice: Theoretical, comparative and transnational perspectives (pp. 7-23). Oxford: Oxford and Portland Oregon.

8 US Legal (2016).High Technology Crime Law and Legal Definition. Retrieved October 6, 2016 from http://definitions.uslegal.com/h/high-technology-crime/

inteligjencës të bazuara në teknologji, të dizajnuara për të luftuar krimin dhe terrorizmin".[9]St Grabosky më shumë se një dekadë e gjysmë më parë parashikoi se përpjekjet e shekullit 21 për të luftuar krimin do të ndihmoheshin shumë nga teknologjia.[10]

Edhe pse "*policimi pa kufi*" nuk është një koncept popullor, ai padyshim kap thelbin e policimit që kërkohet në epokën dixhitale.Teknologjia mundëson kryerjen e llojeve të caktuara të krimit në epokën dixhitale dhe për këtë arsye duhet të nxisë përpjekjet për t'i luftuar ato.Prandaj, zbatimi i ligjit duhet të zhvillojë aftësi superiore teknologjike për të qenë në gjendje të gjurmojë dhe trajtojë krimin e teknologjisë së lartë.

Siguria kibernetike

Është e vështirë të arrihet në një përkufizim përgjithësisht të pranueshëm të konceptit të sigurisë kibernetike.Kjo për shkak se shqetësimet e sigurisë kibernetike kalojnë disa kufij disiplinorë dhe janë konceptuar nga këndvështrime të ndryshme disiplinore.

Sipas Moore dhe Pyn "Siguria kibernetike ka të bëjë me studimin e mbrojtjes së informacionit – të ruajtur dhe përpunuar nga sistemet e bazuara në kompjuter, dhe informacionin privat të cenueshëm ndaj ekspozimit dhe keqpërdorimit të paqëllimshëm[11]. Gordon, Loeb, Lucyshyn dhe Zhou përdorin termin për t'iu referuar mbrojtjes së informacionit të transmetuar përmes internetit ose rrjeteve të tjera kompjuterike.[12] Për Ndubueze, "Siguria kibernetike në përgjithësi përfshin të gjitha përpjekjet e individëve, organizatave ose qeverisë drejt heqjes së të gjitha zbrazëtirave të njohura dhe të parashikuara në infrastrukturën kibernetike që mund të shfrytëzohen nga devijuesit në internet, kriminelët dhe terroristët".[13]

9 Worrall, J. L. (2016). Criminal procedure.(2 Ed.). Boston: Pearson Educational Inc.

10 Grabosky, P. (1998). Technology and crime control. Trends and Issues in Crime and Criminal Justice, 78, 1-6.

11 Moore, T and Pyn, D. (2015).Editorial. Journal of Cybersecurity, 1 – 2. doi: 10.1093/cybsec/tyv001.

12 Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015).Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1 (1), 3 – 17. Doi:10.1093/cybsec/tyv011.

13 Ndubueze, P.N. (2014). Cyber Security and Industrial Development in Digital Nigeria. In D.O. Imbhonopi & U.M. Urim (eds.) Trajectory to Industrial development in Nigeria.(pp. 149 – 160). Ota: Department of Sociology, Covenant University.

1. Qasja teorike për parandalimin

Në literaturën akademike gjendet Teoria e Parandalimit (DT), e cila ofron kuadrin teorik për krimet e teknologjisë së lartë dhe qasjen investigative të tyre. Në vijim të saj termi "deterrence" është gjurmuar te fjala latine "dçterrere"; që do të thotë "të frikësosh nga ose larg[14].

Teoria e parandalimit daton në idetë e mendimtarëve klasikë si Cesare Beccaria dhe Jeremy Bentham.Ata argumentuan se kriminelët duhet të marrin dënimin që meritojnë dhe pohuan se objektivi kryesor i dënimit duhet të jetë parandalimi.

Supozimi është se qeniet njerëzore racionale do të zgjedhin sjellje që prodhon kënaqësi në krahasim me atë që prodhon dhimbje, kështu që dënimi i duhur do të pengojë aktivitetin kriminal.[15]Beccaria argumentoi se parandalimi (si specifik ashtu edhe i përgjithshëm) është qëllimi i vetëm legjitim i dënimit.Parandalimi i veçantë ose specifik shërben për të parandaluar kryerjen e krimit në të ardhmen nga individi i dënuar, ndërsa parandalimi i përgjithshëm përdor ndëshkimin e individëve të veçantë për t'i larguar njerëzit në përgjithësi nga kryerja e krimit.[16]

Teoria e parandalimit është kritikuar për mosnjohjen e faktorëve socialë, ekonomikë dhe politikë që ndikojnë në sjelljen kriminale si papunësia, pabarazia racore, varfëria dhe shpërndarja e pabarabartë e burimeve dhe mundësive.[17]

Teoria e parandalimit konsiderohet e përshtatshme për këtë diskurs sepse ofron një kontekst të besueshëm për të kuptuar shtrirjen e krimit dhe kriminalitetit në hapësirën kibernetike dhe se si të policimi efektivisht. Vlen të përmendet se disa studiues kanë aplikuar teorinë e parandalimit për sigurinë kibernetike.[18]

Aktivitetet e paligjshme në internet lulëzojnë për shkak të supozimit të atyre që ndjekin aktivitete të tilla se ata gjithmonë do të shpëtonin nga krimet e tyre.

---

14 Bendiek, A. and Metzger, T. (2015).Deterrence theory in the cyber-century. Retrieved May 5, 2017 from https://www.swp-berlin.org/fileadmin/contents/ products /arbeitspapiere/ Bendiek-Metzger_WP-Cyberdeterrence.pdf

15 Reid, S.T. (2015). Crime and Criminology (14 Ed.). New York: Wolters Kluwer law & Business.

16 Boom, R.M & Haley, K.N. (2005).Introduction to Criminal Justice. Boston: Mc Graw Hill.

17 Tepperman, L. (2006). Deviance, Crime and Control: Beyond the Straight and Narrow. Ontario: Oxford University Press

18 Bendiek, A. and Metzger, T. (2015).Deterrence theory in the cyber-century. Retrieved May 5, 2017 from https://www.swp-berlin.org/fileadmin/contents/ products /arbeitspapiere/ Bendiek-Metzger_WP-Cyberdeterrence.pdf

Kriminelët kibernetikë shfrytëzojnë dobësitë në rrjetet dhe komunikimet e ndërmjetësuara nga kompjuteri për të kryer sulme me qëllim të keq kundër individëve, organizatave dhe vendeve.Një mënyrë themelore për të dekurajuar sulme të tilla është që organet e zbatimit të ligjit të zhvillojnë aftësitë për t'iu përgjigjur menjëherë atyre duke zbuluar sulmet, gjurmimin e autorëve dhe ndëshkimin e duhur të tyre. Një masë e tillë jo vetëm që do t'i pengojë shkelësit në fjalë nga kryerja e shkeljeve të ngjashme në të ardhmen, por gjithashtu do të dërgojë një notë të fortë paralajmërimi për shkelësit e mundshëm në shoqërinë më të madhe se një krim i tillë nuk paguhet. Por për të qenë në gjendje ta bëjnë këtë, agjencitë e zbatimit të ligjit duhet të përdorin një inteligjencë të bazuar në teknologji dhe një inteligjencë superiore.Kjo është e nevojshme për shkak të natyrës komplekse të krimeve të teknologjisë së lartë.

2. Fusha dhe modelet e krimeve të teknologjisë së lartë

Krimi i teknologjisë së lartë është një nga sfidat më të mëdha me të cilat përballen shtetet moderne.Kjo sfidë është edhe më e frikshme duke pasur parasysh faktin se "në hapësirën kibernetike transnacionale, egziston një mjedis ideal kriminogjen sepse ka objektiva dhe mundësi të bollshme, shkelës shumë të motivuar dhe deri vonë, jo shumë rregullime dhe zbatime".[19]Teknologjia e re e bazuar në kompjuter i lejon kriminelët të veprojnë në një mënyrë më efikase dhe efektive. Hajdutët kibernetikë tani kanë luksin të mbeten anonimë, duke jetuar në çdo pjesë të planetit, duke kryer biznesin e tyre gjatë ditës ose në mbrëmje, duke punuar vetëm ose në grup, ndërsa në të njëjtën kohë arrijnë një numër shumë më të madh viktimash të mundshme sesa ndonjëherë më parë.[20]Teknologjia e informacionit dhe komunikimit (TIK) është një pjesë e domosdoshme e shoqërive moderne pasi shërbimet kritike si sistemet financiare, transporti dhe tregtia varen nga konfidencialiteti, integriteti dhe disponueshmëria e tyre.[21]Bumi në sektorin e TIK po revolucionarizon aktivitetin kriminal dhe po krijon probleme për zbatimin e ligjit.Këto probleme të cilat janë evidente në përdorimin e kompjuterëve në rrjet dhe teknologjive të tjera në kryerjen e krimit janë të përhapura.[22]

19 Smith, R.G., Grabosky, P. and Urbas, G. (2004).Cyber criminals on trial. Cambridge: Cambridge University Press.

20 Siegel, L. J. (2009). Essentials of criminal justice.(6 Ed.). USA: Wadsworth Cengage Learning.

21 Vidali, A. (2009). Striking the balance: Security vs. Utility.In U. Gori (Ed.).Modelling cyber security: approaches, models, strategies. (pp. 11-28). Amsterdam: IOS Press.

22 Sussmann, M. (1999).The critical challenges from interpersonal high-tech and computerrelated

Krimi kibernetik mbështetet në teknologjitë dixhitale si kompjuterët, teknologjitë e komunikimit dhe shërbimet në rrjet .[23]Ka informacione në lidhje me objektivat e mallrave për sulm në internet dhe informacione të tilla përcaktojnë llojin e taktikave dhe armëve kibernetike që do të përdoren për të shfrytëzuar dobësitë në rrjetin kompjuterik. Agjencitë e zbatimit të ligjit janë të mendimit se më shumë banda të organizuara kriminale po rrethojnë hapësirën kibernetike; duke u motivuar nga paratë e fituara nga grupet e tjera nga sulmet DDos të drejtuara nga phishing dhe zhvatje.[24]Gjithashtu, qeveria, agjencitë e zbatimit të ligjit, akademikët si dhe industria e sigurisë kibernetike besojnë se grupet konvencionale të krimit të organizuar tani po kryejnë krimin dixhital.[25] Në gusht të vitit 2008, prokurorët federalë të Shteteve të Bashkuara akuzuan 11 të dyshuar nga Estonia, Ukraina, Kina, Bjellorusia dhe Shtetet e Bashkuara, të cilët dyshohet se vodhën dhe shitën 40 milionë numra të kartave të kreditit dhe debitit pasi kishin hakuar në rrjetet ËiFi dhe instaluar programe "sniffer". përmes të cilave ata aksesonin numrat dhe fjalëkalimet e kartave (Reid, 2015).

Bandat kanë rrethuar edhe internetin.Është argumentuar se rrjetet sociale u mundësojnë bandave të zgjerojnë bazën e tyre të rekrutimit për anëtarët e bandave dhe të shtohen me tregjet e reja pushtuese.[26] Ngacmimi dhe ndjekja seksuale kanë marrë një dimension krejt të ri në internet. [27]Ekziston gjithashtu sfida e aksesit publik në faqet e internetit të paligjshme.Këto faqe interneti përpiqen të shmangin zbulimin nga agjencitë e kontrollit dhe kjo arrihet duke adoptuar disa taktika mbijetese si mbyllja e gradave, përdorimi i fjalëkalimeve për aksesin në grupet e lajmeve dhe përdorimi i ri-mailerëve, serverëve anonimë dhe mashtrimit të protokollit të internetit.[28]Pirateria e muzikës që është shkarkimi i paautorizuar i muzikës është një problem në rritje.Sipas Shoqatës së Industrisë Regjistruese të Amerikës, vetëm 37

crime at the millennium.Duke Journal of Comparative and International Law, 9 (451), 451 -489.

23 Smith, R.G., Grabosky, P. and Urbas, G. (2004).Cyber criminals on trial. Cambridge: Cambridge University Press.

24 Warren, P. and Streater, M. (2005). Cyber alert: How the world is under attack from a new form of crime.London: Vision paperback.

25 Broadhurst, R., Grabbosky, P. Alazab, M. and Cohen, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8 (1), 1-20.

26 Haut, F. (2014). Cyberbanging: When criminal reality and virtual reality meet. International Journal of Criminology, 2 (2), 20-27.

27 Yar, M. (2013). The policing of internet sex offences: Pluralized governance versus hierarchies of standing. Police and Society, 23 (4), 482 – 497

28 Westluke, B.G. and Bochard, M. (2015). Criminal careers in cyberspace: Examining websites failure within child exploitation networks. Justice Quarterly. DOI: 10.1080/07418825.2015.1046393.

% muzikës u blenë në mënyrë legjitime në 2009.[29] Deklarata e Samitit Ndërkombëtar të Bangkok (2007) mbi Policimin e Hapësirës Kibernetike identifikoi tendencat dhe teknologjitë/malëare në të ardhmen në zhvillim:

- Spyëare që fshihen pas rootkits;
- Zhvillimi i regjistruesve kryesorë;
- Certifikata dixhitale false;
- Sulmet e konfigurimit të rrjetit (mirco në makro) për të ridrejtuar trafikun në ueb/email;
- Malëare vetë-morfues;
- Infeksion përmes rrjetit peer to peer (Myspace, YouTube, Facebook);
- Sulmi i bazuar në skript për web 2.0;
- Shfrytëzimet nga ana e klientit që zgjerohen nga shfletuesi i internetit në Word, Excel dhe PowerPoint;
- Zero day exploits në makrot e ëord dhe excel;
- Sulmi i përshkallëzimit të privilegjeve në makinat jo-Vista;
- Botnet vërtet të mëdha (superkompjuter në zotërim të kriminelëve);
- Kalimi në platformën celulare, PDA dhe iPod, iPhone.[30]

Krimi i teknologjisë së lartë po rritet në mënyrë dramatike në të gjithë globin. Sipas McAfee Labs Threat Report (2016), mbi 157 milionë përpjekje janë bërë çdo ditë përmes emailit, kërkimeve në shfletues etj. për të joshur klientët e saj për t'u lidhur me URL-të e rrezikshme. [31]Mbi 353 milionë skedarë të infektuar shënjestroheshin në rrjetet e klientëve të saj çdo ditë. Gjithashtu, 71 milionë programe të padëshiruara përpiqen të instalojnë ose lëshojnë vetë çdo ditë.Për më tepër, 55 milionë përpjekje janë bërë nga klientët e saj për t'u lidhur me adresat e rrezikshme të protokollit të internetit (IP) ose adresa të tilla përpiqen të lidhen me rrjetet e klientëve të tyre. Në mënyrë të ngjashme, Symantec Internet Security Threat Report (2016) zbulon se Symantec zbuloi mbi 430 milionë lloje unike të malëare në 2015 (duke

29 Marcum, C.D. (2014). Cyber Crime. New York: Wolters Kluwer.

30 Jaishankar, K. Pamg, B and Hyde, S. (2008). Bangkok International Summit (2007). Declaration of policing cyberspace: International Journal of Cyber Criminology. 2 (1): 256 – 270.

31 McAfee Labs Threat Report (2016).
Retrieved October 2, 2016 from http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar2016.pdf

treguar një rritje prej 36 përqind nga 2014).[32] Më tej raporton se më shumë se gjysmë miliardë të dhëna personale janë vjedhur ose humbur në 2015 dhe 191 milionë të dhëna janë ekspozuar në një nga shkeljet më të mëdha të të dhënave në botë, ndërsa janë ekspozuar 429 milionë identitete. Qendra e Raportimit të Krimit në Internet në raportin e saj të krimit në internet të vitit 2015 ofron një pasqyrë më të thellë mbi shtrirjen dhe modelet e krimeve të teknologjisë së lartë. Sipas raportit, janë raportuar 1,070,711,522 dollarë humbje, janë pranuar 288,012 ankesa dhe kanë raportuar humbje 127,145 ankesa. Raporti zbulon gjithashtu se në vitin 2015, 5 vendet kryesore sipas vendndodhjes së viktimave ishin: Shtetet e Bashkuara (80.2%), Mbretëria e Bashkuar (2.47%), Nigeria (2.2%), Kina (1.91%) dhe India (1.46%). 5 llojet kryesore të krimit përfshinin: Kompromisi me email të bizneseve (246, 226, 016 dollarë),Mashtrimi i besimit/Romanca (203, 390, 531 dollarë), Mospagesa/mosdorëzimi (121, 329, 122 dollarë), Investime (119, 177, 899 dollarë), Vjedhja e identitetit (57, 204, 589 dollarë, Raporti) 2015

Teknologjia dhe Policimi përmës saj imkrimeve

Teknologjia krijon mundësi të jashtëzakonshme biznesi.Ai gjithashtu krijon modele të reja të krimit dhe strategji të reja policie për kontrollin e krimit.Teknologjia është përcaktuar si "tërësia e njohurive dhe teknikave që njerëzit përdorin për të krijuar objektin material të jetesës dhe rehatisë së tyre".[33]Elementët kriminalë historikisht kanë shfrytëzuar maksimalisht teknologjinë në sipërmarrjen e tyre.

Kjo është ndoshta arsyeja pse argumentohet se: Aktorët e paligjshëm ekonomikë, jo-shtetërorë, transnacionalë, duke filluar nga trafikantët e drogës tek pastruesit e parave e deri te tregtarët e armëve të tregut të zi, shpesh përshkruhen si gjithnjë e më të shkathët, të sofistikuar, sfidues të kufijve dhe të zgjuar teknologjikisht. Shtetet, në kontrast të mprehtë, zakonisht përshkruhen si gjithnjë e më shumë të rrethuara, të zgjuara, të pajisura keq, të ngathët dhe madje të paaftë në trajtimin e anës së paligjshme të globalizimit.[34] Megjithatë, agjencitë e zbatimit të ligjit nuk po heqin dorë në përpjekjet e

32 McAfee Labs Threat Report (2016).
Retrieved October 2, 2016 from http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar2016.pdf

33 Walsh, A. and Hemmens, C. (2014). Law, Justice and Society: ASociological Introduction, rd (3 ed.). New York: Oxford University Press.

34 Andreas, P. (2015). Illicit globalization myths and misconceptions. V. Mitsilegas, P. Alldridge and L. Cheliotis (eds.). Globalization, Criminal Law and Criminal Justice: Theoretical, Comparative and Transnational Perspectives, (pp. 45 – 64). Oxford: Hart Publishing.

tyre për të përqafuar teknologjitë në zhvillim dhe për të ripozicionuar më mirë veten për një goditje ndaj organizatave dhe aktiviteteve kriminale. Theksohet se: Roli i teknologjive të reja në lehtësimin e zbatimit të ligjit ka ardhur, nëse ka ardhur në rritje. Për shembull, edhe pse teknologjitë e reja të informacionit mundësojnë krimin ndërkufitar, këto përparime teknologjike gjithashtu rrisin në masë të madhe kapacitetet e gjurmimit dhe mbikëqyrjes, shumë përtej përgjimeve tradicionale.Teknologjia gjithashtu ka ulur në mënyrë dramatike kostot dhe ka rritur intensitetin dhe frekuencën e rrjeteve ndërqeveritare të zbatimit të ligjit.Shkurtimisht, shumë nga të njëjtat transformime teknologjike që lehtësojnë globalizimin e krimit lehtësojnë gjithashtu globalizimin e kontrollit të krimit.[35] Byrne dhe Marx [36]i ndajnë risitë në teknologjinë e drejtësisë penale në dy kategori të gjera, përkatësisht: teknologji e vështirë; që përfshin harduerin ose materialet dhe teknologjinë e butë që përbëhet nga programet kompjuterike dhe sistemet e informacionit. Ata më tej vërejnë se risitë e vështira të teknologjisë përfshijnë materiale, pajisje dhe pajisje të reja që mund të përdoren ose për të kryer krime ose për ta parandaluar atë. Ata identifikojnë shembuj të teknologjive të vështira të përdorura për të parandaluar krimin, duke përfshirë: Kamerat e televizionit me qark të ngushtë (CCTV), detektorët e metaleve, pajisjet e kontrollit të bagazheve si dhe pajisjet që mund të përdoren për të kryer ose parandaluar krimin. Ato të vendosura nga policia përfshijnë armë të reja, pajisje më pak se vdekjeprurëse, makina të reja patrullimi të përmirësuara me teknologji si dhe pajisje mbrojtëse policore.Teknologjitë e buta në thelb përfshijnë përdorimin e informacionit për të parandaluar krimin.Shembujt përfshijnë teknologjinë parashikuese të policisë dhe mekanizmat e regjistrimit/ transmetimit të videos në automjetet e policisë.Programet e reja softuerike, sistemet e klasifikimit, metodat e analizës së krimit si dhe sistemi i ndarjes së të dhënave/integrimit të sistemit janë identifikuar të gjitha si inovacione të teknologjisë së butë.[37]

Argumentohet se sa më shumë një shoqëri të bëhet teknologjikisht e avancuar, aq më shumë ndërfaqja ndërmjet pjesëve të saj bëhet komplekse,

35 Andreas, P. (2015). Illicit globalization myths and misconceptions. V. Mitsilegas, P. Alldridge and L. Cheliotis (eds.). Globalization, Criminal Law and Criminal Justice: Theoretical, Comparative and Transnational Perspectives, (pp. 45 – 64). Oxford: Hart Publishing.

36 Byre, J. & Marx, G. (2011). Technological innovations in crime prevention and policing: A Review of the research on implementation and impact. Cahiers Politiestudies Jaargang, 3 (20): 17-40

37 Byre, J. & Marx, G. (2011). Technological innovations in crime prevention and policing: A Review of the research on implementation and impact. Cahiers Politiestudies Jaargang, 3 (20): 17-40

duke kërkuar kështu nevojën për të rregulluar ndërfaqen.[38]Ndryshimet teknologjike rritën profesionalizmin e policisë.[39]Teknologjitë biometrike si printimi dixhital i gishtave, njohja e fytyrës, skanimi i irisit dhe profilizimi i acidit deoksiribonukleik (ADN) midis një morie teknologjish të tjera po evoluojnë dhe po përdoren gjithnjë e më shumë në polici.Gjithashtu, në policimin bashkëkohor përdoret përgjimi elektronik, i cili është përshkruar si metoda të ndryshme të përdorura për të spiunuar aktivitetet e të dyshuarve për krime, si përgjimet, përgjimet, hakerimet në transmetimet kompjuterike, gjurmimi i lëvizjeve të njerëzve dhe pajisjeve, mbikëqyrja video, përdorimi i imazheve termike dhe detektorë armësh[40]. Provat e ADN-së mund të përcaktojnë kryerjen e një krimi, elementët e tij bazë/dëshminë e dëshmitarëve, të implikojnë ose të shfajësojnë disa në krim .[41]

3. Sfidat në investigimin e krimeve të larta teknologjike

Hetimi është një proces diskret i cili do të udhëhiqej me nivelin më të lartë të konfidencialitetit.

Praktikisht, kjo është kërkesa përfundimtare, por përvoja sugjeron se rastet e rënda mund të hyjnë në hetim dhe të përpiqen të prishin rrjedhën e tij. Komuniteti modern i sigurisë dhe inteligjencës do të merrej me një zbulim të tillë dhe do të përdorte mjekësinë ligjore kibernetike për të gjurmuar rrugën e kriminelëve. Synimi përfundimtar i hetimit është të merren sa më shumë gjetje dhe prova që të munden dhe të arrestohen të gjithë aktorët keqdashës të përfshirë në krimet e rënda.

Gjatë historisë, krimi do të kalojë nëpër shumë faza - ai do të lidhej më së shumti me fushën fizike dhe do të përdorte armët e përshtatshme për një periudhë të zhvillimit të njeriut për kryerjen e veprave të rënda, por sot do të kalonte me shpejtësi në një hapësirë kibernetike. Për momentin, ne nuk jemi plotësisht në epokën kibernetike që flet për krimin. Kjo fazë mund të përshkruhet si një kalim nga epoka fizike në atë kibernetike lidhur me veprat penale. Tendenca aktuale sugjeron që shumë shpejt bankat nuk do ta bënintë

38 Walsh, A. and Hemmens, C. (2014). Law, Justice and Society: ASociological Introduction, rd (3 ed.). New York: Oxford University Press.

39 Uchida, C.D. (2015). Ahistory of American policing. In M. Maguire and D. Okada (eds.). nd Critical issues in crime and justice: Thought, policy and practice, (2 Ed.). (pp. 245 – 257). Los Angeles: Sage Publications.

40 Worrall, J. L. (2016). Criminal procedure.(2 Ed.). Boston: Pearson Educational Inc.

41 Michaelis, R.C. , Fkanders, Jr. and Wulff, P.H. (2008). Alitigator's guide to DNA: From the laboratory to the court room. Amsterdam: Elsevier Academic Press.

grabiten nga brenda duke përdorur armë dhe logjistikë të mirëorganizuar, por më tepër nga jashtë duke përdorur teknologjitë në distancë. Pra, padyshim që ne po kalojmë nga një epokë e krimit të orientuar fizikisht në epokën kibernetike të veprave penale, që do të thotë se kjo kohë e re me kriminologjinë kërkon aftësi dhe ekspertizë të reja nga stafi i mbrojtjes që të jetë në gjendje t'i përgjigjet sfidave të kësaj epoke të re.Krimet e lidhura me seksin mund të përfshijnë përdhunimin, prostitucionin, pedofilinë, pornografinë dhe shumë më tepër.[42]Këto lloj veprash penale janë të ndërlidhura në mënyrë të moderuar me përdorimin e teknologjive kibernetike.Nëpërmjet kërkimit tonë teorik, ne do të merrnim disa informacione të dobishme se si funksionon krimi i organizuar dhe se si ai është i varur nga një teknologji e re.

Siç dihet, krimet e lidhura me drogën janë veprat penale më të rënda për shkak të buxhetit të madh me të cilin merret organizata kriminale.[43] Ky lloj biznesi kriminal mund të jetë një kërcënim serioz për Sistemin Ligjor si dhe për Forcat e Mbrojtjes, sepse nëpërmjet fondeve të tyre - ato mund të sponsorizojnë kërcënimet e sigurisë shumë konkurruese, të cilat do të ishin kundër gjithçkaje ligjore, do të luftonin për zotërit e tyre të drogës dhe do të përpiqeshin të bëj një grusht shumë vendeve dhe qeverive të tyre. Ndonjëherë bandat do të përdornin kriminelët kibernetikë me disa aftësi hakerimi për të gjurmuar viktimat dhe për të marrë më shumë informacion rreth tyre përmes ndjekjes në internet ose fizike. Shumë nga këto raste ashtu si trafikimi i qenieve njerëzore mund të lidhen me skenarët e rrëmbimit të koordinuara me kujdes duke përdorur teknikat e gjurmimit kibernetik.[44] Viktimat e trafikimit të qenieve njerëzore normalisht nuk kanë të drejta njerëzore dhe ato thjesht detyrohen të shfrytëzohen fizikisht, seksualisht ose mendërisht. Së fundi, rastet e rënda si vrasjet dhe krimet e lidhura me armët mund të jenë mesatarisht të lidhura me aplikimin e teknologjive në zhvillim. Rastet e armëve mund të përfshijnë kontrabandën dhe përdorimin e armëve të zjarrit. Është e qartë se ky lloj i veprave penale ka nevojë për punën e rrjetit të mirë, kështu që mund të përdoren një lloj kapaciteti komunikimi duke i ndërlidhur këto edhe me teknologjitë kibernetike. Aftësitë e hakerëve janë gjithashtu të mirëseardhura brenda një organizate të tillë për arsye të

42 Delgado A, Ensuring our Children's Safety While Connected, The US Air Force Central Command, 2015, [Internet], The WEB source: http://www.-afcent.af.mil/Units/379thAirExpeditionaryWing/Ne ws/Display/tabid/298/Article/622136/ensuring-ourchildrens-safety-while-connected.aspx

43 Omari A, Al-Kasasbeh B, Al-Qutaish R, Muhairat M. DEA-RTA: A Dynamic Encryption Algorithm for the Real-Time Applications, International journal of computers, Vol. 3, Issue 1, pp. 191-199, 2009.

44 Peterson M, Intelligence-Led Policing: The New Intelligence Architecture, Bureau of Justice Assistance, 2005

marrjes së dokumenteve false për kalimin e paprekur të kufijve. Shumë nga grupet e krimit të organizuar do të kishin anëtarët ndërkombëtarë që bëjnë një organizatë të tillë me karakter transnacional.

Hetuesit dhe prokurorët luftojnë për të gjetur prova të mjaftueshme për ndjekjen penale të krimit kibernetik.Përveç sfidave të shumta juridiksionale në hetimet e krimit kibernetik, teknologjia dhe rrjedha e punës e hetimit paraqesin disa sfida për hetimin dhe ndjekjen penale të krimit kibernetik.[45]

- Investimi i kohës: Hetimi i krimit kibernetik sjell sfida unike të cilat nuk hasen në shumicën e hetimeve tradicionale të krimit. Ndërsa hetimi tradicional i krimit nuk kërkon investime paraprake në kohë, megjithatë mund të çojë në arrestimin e kriminelit, hetimet e krimit kibernetik kërkojnë një investim kohe, por mund të rezultojnë në asnjë arrestim. Koha e parashikuar për krimin atipik kibernetik është disa muaj dhe vite në varësi të natyrës së krimit të kryer.

- Puna me viktimat: Hetimi i krimeve kibernetike përfshin punën me viktimat gjatë procesit të hetimit. Gjatë hetimeve, agjentët e zbatimit të ligjit (hetuesit) punojnë me pronarët ose kujdestarët e sistemit të sulmuar për të kuptuar më thellë incidentin. Kur një organizatë sulmohet, hetuesit mbështeten te individët në organizatë për të marrë një informacion të detajuar rreth krimit. Shumica e viktimave nuk do të donin të përfshiheshin në hetimet e krimit kibernetik nga frika e sulmeve të mëtejshme.

- Rrjedha e punës së hetimit: Ndjekja tradicionale e krimit ndodh horizontalisht ndërsa hetimi dhe ndjekja e krimit kibernetik janë një përzierje e proceseve horizontale dhe vertikale - në varësi të disponueshmërisë së ekspertizës dhe teknologjisë për hetim. Për shembull, në hetimet dhe ndjekjen penale tradicionale të krimit, zyra të ndryshme avokatësh trajtojnë detyra të ndryshme në mënyrë të njëpasnjëshme derisa çështja t'i kalojë atij që është përgjegjës për gjykimet dhe procedurat e dënimit. Hetimi dhe ndjekja penale e krimit kibernetik, për shkak të natyrës së specializuar të hetimeve të krimit kibernetik nuk trajtohet gjithmonë në mënyrë sekuenciale.

- Teknologji dhe ekspertizë e ulët: Natyra teknike e krimit kibernetik e bën këtë qasje pothuajse të pamundur. Për shkak të natyrës teknike të krimit kibernetik, përfshihen vetëm prokurorët që mund të trajtojnë krimin kibernetik.Për më tepër, krimi kibernetik mund të automatizohet në një mënyrë që një krim tradicional nuk mundet. Si rezultat, agjencitë e zbatimit të ligjit janë të detyruara të japin përparësi dhe të hetojnë krimet më të rënda

45 Samuel Owusu – Cybersecurity Specialist (Advanced Evidence Discovery Ltd and Institute of Cybersecurity, Ghana).Member, Institute of ICT Professionals Ghana

. Aftësitë e nivelit të ulët të kompjuterëve midis punonjësve të zbatimit të ligjit dhe prokurorëve është një nga sfidat teknologjike me të cilat përballen agjentët e zbatimit të ligjit në hetimin dhe ndjekjen penale të kriminelëve kibernetikë.

- Pajisjet e mjekësisë ligjore dixhitale: Hetimi dhe ndjekja penale e krimit kibernetik gjithashtu kërkon disa pajisje të cilat u mungojnë shumicës së zyrave të zbatimit të ligjit. Mjetet dhe aksesorët e mjekësisë ligjore dixhitale, laboratorët kompjuterikë, pajisjet e regjistrimit dhe materialet e ruajtjes janë disa nga pajisjet që agjencitë ligjzbatuese kanë nevojë për të kryer aktivitete hetimore, por shumë pak qendra të zbatimit të ligjit janë të pajisura me këto teknologji.

- Ekspertiza e krimit kibernetik: Gjetja e ekspertëve të krimit kibernetik për të kryer hetime dhe ndjekje penale të krimit kibernetik kërkon investim në kohë dhe para. Shumica e ekspertëve të mjekësisë ligjore dixhitale punësohen për të punuar si punonjës me kohë të plotë, por menaxherët e punësimit priren t'i humbasin sepse menaxhmenti nuk i plotëson nevojat e tyre, duke përfshirë trajnimin dhe nevojat e pajisjeve.[46]

Çfarë mund të përmisohet në procesin e investigimi të krimeve kibernetike?[47]

Zhvillimi i burimeve njerëzore të krimit kibernetik: Zhvillimi i burimeve njerëzore për hetimin e krimit kibernetik midis agjencive të zbatimit të ligjit është shumë i rëndësishëm. Meqenëse është e vështirë të rekrutohen ekspertë të krimit kibernetik, është e rëndësishme që qeveria të zhvillojë ekspertizën e krimit kibernetik në disa nga oficerët ekzistues të zbatimit të ligjit. Meqenëse jo çdo oficer i zbatimit të ligjit mund të zhvillojë aftësitë e nevojshme për hetimin e krimit kibernetik, është e rëndësishme që qeveria të zgjedhë vetëm ata që janë të përshtatshëm për hetimet e krimit kibernetik. Është humbje burimesh të trajnosh çdo oficer policie për hetimin e krimit kibernetik. Një mjet që ndihmon në përzgjedhjen e atyre që janë të përshtatshëm për zhvillimin profesional të krimit kibernetik është anketa. Anketa i mundëson menaxhmentit të identifikojë hetuesit dhe prokurorët që kanë interes në kryerjen e hetimit dhe ndjekjes penale të krimit kibernetik.

46 Samuel Owusu – Cybersecurity Specialist (Advanced Evidence Discovery Ltd and Institute of Cybersecurity, Ghana). Member, Institute of ICT Professionals Ghana

47 Samuel Owusu – Cybersecurity Specialist (Advanced Evidence Discovery Ltd and Institute of Cybersecurity, Ghana). Member, Institute of ICT Professionals Ghana

Takimet individuale duhet të mbahen me njerëz që kanë aftësi themelore të hetimit të krimit kibernetik për orientim dhe motivim në karrierë. Individët e përzgjedhur për hetime dhe ndjekje penale të krimit kibernetik më pas kalojnë nëpër të paktën trajnime bazë për hetimin e krimit kibernetik. Ata që kanë një interes të madh duhet të sponsorizohen për t'u trajnuar në kurse të avancuara të krimit kibernetik.

Krijimi i njësive të krimit kibernetik: Zyrat e zbatimit të ligjit duhet të krijojnë njësi të krimit kibernetik në rajone kryesore me qëllim dhe përgjegjësinë e trajtimit të hetimeve të krimit kibernetik dhe përgjegjësive të ndjekjes penale në nivele rajonale. Menaxhmenti duhet të sigurojë që stafi i caktuar për hetimin e krimit kibernetik dhe ata që mbështesin hetuesit marrin trajnim dhe zhvillim.Një trajnim i vazhdueshëm në shërbim për ekipin është shumë kritik. Hetuesit duhet të vazhdojnë trajnimin dhe zhvillimin profesional në këtë temë për të mbajtur krah për krah me trendet më aktuale të krimit kibernetik dhe hetimeve.

Blerja e pajisjeve hetimore: Pajisjet hetimore të cilat janë lehtësisht të aksesueshme dhe janë të lehta për t'u përdorur, nevojiten për të drejtuar njësitë e krimit kibernetik. Për hetime efikase, zyrat e zbatimit të ligjit duhet të pajisen me pajisje hetimore.Pajisjet e nevojshme për hetimet e krimit kibernetik janë hardueri kompjuterik, aksesorët kompjuterikë dhe aksesorët për softuerin dixhital të mjekësisë ligjore dhe mjekoligjore.Njësitë e zbatimit të ligjit për krimin kibernetik mund të kërkojnë ndihmë nga kompani private dhe filantropë ose agjenci të tjera qeveritare. Njësia duhet të kontaktojë shitësit e softuerit të mjekësisë ligjore për blerje dhe mbështetje të softuerit të lire.

Përdorimi i hetuesve privatë të sigurisë: Kur një krim është kompleks dhe kërkon ekspertizë dhe shërbime të avancuara, qeveria dhe organizatat dhe individët e prekur mbështeten në ekspertizën e hetuesve privatë të krimit kibernetik si Advancedevidence.com për të përmbushur nevojat e hetimeve të krimit kibernetik.

Konkluzione

Teknologjia ka ndikuar gjithmonë në shtrirjen dhe modelet e krimit dhe kriminalitetit në mbarë botën.Ndërsa teknologjia bëhet e sofistikuar, po ashtu bëhet edhe krimi dhe kriminaliteti. Për fat të keq, megjithatë, kriminelët kanë përqafuar gjithmonë teknologjinë e lartë më shpejt se zbatimi i ligjit. Sofistikimi në rritje i krimit të teknologjisë së lartë në të gjithë botën,

nënvizon qartë nevojën për një ndryshim paradigme në polici.Policia pa kufij në thelb përfshin përdorimin e inteligjencës së orientuar nga teknologjia në trajtimin e problemit të krimit dhe terrorizmit.Ky dokument argumentoi se policimi pa kufi do të shërbejë si një strategji efektive për kontrollin e krimeve të teknologjisë së lartë. Meqenëse krimet e lidhura me kompjuterin dhe internetin ndihmohen nga teknologjia, ato do të kërkojnë një strategji të orientuar drejt teknologjisë për t'u kontrolluar dhe menaxhuar.

Bibliografia

1. Behl A, Behl K, An Analysis of Cloud Computing Security Issues, In Proc. 2012 World Congress on Information and Communication Technologies, IEEE, Trivandrum, India, pp. 109-114, 30 Oct.-2 Nov. 2012.
2. Charney S, Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft Corp., 2009.
3. Delgado A, Ensuring our Children's Safety While Connected, The US Air Force Central Command, 2015, [Internet], The WEB source: http://www.- afcent.af.mil/Units/379thAirExpeditionaryWing/News/Display/tabid/298/Article/622136/ensuring-ourchildrens-safety-while-connected.aspx
4. Booz Allen Hamilton, Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity, 2011.
5. Jason H, Cloud Attack: Unsharing Your Business in The Cloud, BrightTALK, 2015.
6. Khalil I. M, Khreishah A, Bouktif S, Ahmad A, Security Concerns in Cloud Computing, In Proc. 10th International Conference on Information Technology: New Generations, pp. 411-416, Las Vegas, NV, USA, 2013.
7. Siegel, L.J. (2009). Essentials of criminal justice (6 Ed.). Australia: Wadsworth Cengage Learning.
8. Smith, R.G. (2014). Transnational cybercrime and fraud.In Reichel, P. and Albanese, J. nd (Eds.).Handbook of transnational crime and justice (2 Ed.).(pp. 119- 142). Los Angeles: SAGE Publications. 9.Mallicoat, S.L. (2014). The politics of crime and the policy of making process.In S.L. Mallicoat and C.L. Gardiner (Eds).Criminal Justice Policy. (pp.1-

14). Los Angeles: Sage Publications Inc.

10. Marcum, C.D. (2014). Cyber Crime. New York: Wolters Kluwer.
11. Martin, A.K. and Whitely, E.A. (2013). Fixing identity? Biometrics and the tensions of material practices. Media Culture and Society, 35 (1), 52 – 60.
12. McAfee Labs Threat Report (2016). Retrieved October 2, 2016 from http://www.mcafee.com/u

NOW I SEE YOU: HOW TO BYPASS THE E2EE CONUNDRUM AND IDENTIFY PERSONS IN A CYBERCRIME ENVIRONMENT?

LLM. ILVANA DEDJA

Legal researcher

Faculty of Law, University of Tirana

ilvanadedja1@gmail.com

I. Introduction

Cyberspace is a combination of 1s and 0s, that create a unique dimension where humans live, work and profit in/from it. The word "cyber" itself, implies a set of rules different from the real world.[1] This misconception has made people believe that there are grey areas left for suspicious activity in the cyberspace where you can manage to "break the law".[2] As the cyberspace exponentially expands and increases its influence in the real world, there is a necessity to work on this misconception.

The dilemma with cyberspace is that it was not thought to be a *mala in se* environment that facilitates crime. Nonetheless, the human found ways to use the virtual reality to commit crimes within it, or even use it to do so in the real world. Clough explains this phenomenon in the sense that the scale of the potential offenders and victims on the internet (approximately 40 per cent of the world), who have access in online marketplaces, or the Dark Web, and can hide behind proxy servers, make the perfect environment

1 Adrian Mihalache, The Cyber Space-Time Continuum: Meaning and Metaphor (2002) The Information Society, DOI: 10.1080/01972240290075138.

2 Interpol, Cybercrime, https://www.interpol.int/en/Crimes/Cybercrime, all links are last accessed by 15 June 2022.

for conducting cyber offences.[3] The Dark Web facilitates the sale of drugs, firearms, stolen data, and child exploitive material. In an investigation of these marketplaces, 61 individuals from 17 countries were arrested for using the Dark Web to sell counterfeit goods, cybercrime services, human trafficking, and drugs.[4]

VPNs,[5] TORs[6], and End-to-end encryption[7] are technologies not necessarily reserved for the crimes offenders.[8] As a result, the legal community is divided in two camps: One that argue the need for governments and law enforcement agencies to have access to such technologies, or either ban them altogether, or the other that argue in favour that these technologies are imperative for the protection of the right of privacy in cyberspace. As the debate has reached an impasse, a theoretical approach is to finds innovative solutions to the encryption and anonymity issue.

The impetus for this paper was provided by the dispute over whether End-to-End encryption, and other anonymity tools, ought to be criminalized as technologies that are facilitating crime. This essay goes beyond this dilemma and draws on the work of criminologist and members of STEM field to what other options there are for law enforcement agencies to discover the identity of someone who commits a cybercrime. At first, it provides a brief context of the problem of encryption, as a "safe haven" for criminals committing cyber-enabled crimes. Then, it tries to clarify the notion of identity in connection with the virtual world, and how does cyberprofiling might help law enforcement agencies (LEAs) to tackle crime. At last, it provides possible solutions to this problem, including forcing Internet Service Providers (ISP) to use backdoors and making use of metadata. Continuously, this essay explores the importance of international cooperation, in particular to crimes that transcend borders and leave data or traces in more than one jurisdiction.

3 Jonathan Clough, Principles of Cybercrime (2015), 2nd Edt. Cambridge Pres, p 239.

4 Thomas J Holt and Adam M Bossler, 'An Assessment of the Current State of Cybercrime Scholarship' (2014) 35 Deviant Behavior 20.

5 VPN is a virtual private network

6 Tor is an open-source software that permits users to access the Internet through a series of virtual servers without making a direct connection.

7 End-to-end encryption is a system of communication where only the communicating users can read the messages. See more Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). Front Matter. In The Effect of Encryption on Lawful Access to Communications and Data (p. I–II). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep23146.1.

8 Holt (n 4) p 93.

II. Cyber-enabled crime, data, and the digital footprint

In a cyberspace environment, a perpetrator is either going to commit new crimes, based on digital advancement, or exploit existing technologies to commit traditional crimes.[9] Correspondingly, cybercrime as a crime that involves a computer, can be either cyber-dependent offences[10] or cyber-enabled offences.[11] Cyber-enabled crimes are defined as traditional crimes that can be committed without the use of information communication technology, but whose consequence or reach is enabled by a computer.[12] In such circumstances, fraud, intellectual property crime, violence against women and girls, or child sexual offences are traditional crimes that through the use of technology, browsing illegal online markets or social engineering techniques, the scale and nature of the crime aggravates.

Considering the growing prominence of crime in cyberspace, the Budapest Convention[13] attempts to provide a unified front against cybercriminals. The Cybercrime Convention, which is structured in three distinctive parts, first, the part that harmonises the specific cybercrime offences with the aim to help states to corporate in investigation; second, the part that dwells into the minimum investigation powers of law enforcement authorities, and the third part, which focuses on Mutual Legal Assistance and how it works, serves as an instrument for international cooperation in solving cross border cybercrimes.[14] From the perspective of law, adopting the Cybercrime Convention results in new laws that regulate information systems and investigators powers. In the UK, the Investigatory Powers Act governs how law enforcement agencies can acquire lawfully communication data about who, where, when and with whom a communication happened.[15] In

9 Di Nicola, A. Towards digital organized crime and digital sociology of organized crime. Trends Organ Crim (2022), https://doi.org/10.1007/s12117-022-09457-y.

10 UNODC, Global Programme on Cybercrime, Cyber-dependent crime requires an ICT infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack), https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

11 Clough (n 3) p 11.

12 Home Office UK, Cyber crime: A review of the evidence, Research Report, (2013) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf, last accessed 15 June 2022.

13 Council of Europe Convention on Cybercrime, ETS No 185 (Brussels, 23 November 2001, entered in force 1 July 2004) (hereafter Cybercrime Convention).

14 Cybercrime Convention.

15 Investigatory Powers Act 2016.

the US, the Computer Fraud and Abuse Act (CFAA)[16] governs cases where computers are used to commit crimes. Whereas in Albania, the legislative power revisited the Albanian Penal Code and added provisions in accordance with the fight against cybercrime.[17] Concretely, there are gaps relating to how Albanian LEAs will cooperate with internet service provider and a comprehensive overview of the specific investigative powers relating to cybercrime, in contrast with the models of the UK and US.

On another note, to both explore and provide a conceptual account of the link between traditional crimes like drug trafficking and the cyberspace, we need to elaborate on the notions of data and the digital footprint. First, data can be understood as every bit of information we leave behind as soon as we are connected in a computer.[18] For example, if someone is part of a criminal organization, and they use phones to send messages to each-other on locations where to pick-up the drugs - the messages, the location, date and time, the user and the content are reflected as data in cyberspace.[19] Further, this data can be data in rest[20] and data in transmission[21], depending whether the message has achieved the end-point or not. It can either be data - information on the computer memory, or metadata - relevant information about the data.[22]

The problem is that there is an abundance of intelligence, which LEA have a difficulty to choose and find on the relevance to prosecute a crime. Subsequently, encryption technology facilitates the communications, plans and executions of such strategies by offenders - making it close to impossible to raise a case in court on the crime they have committed.

16 18 U.S.C S 1030.

17 Law no.10023, dated on 27.11.20082, and Law no. 10054, dated 29.12.2008, see generally Shkembi, A., Shtupi, I., & Qafa, A. (2016). The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation. Academic Journal of Interdisciplinary Studies, 5(1), 127. Retrieved from https://www.richtmann.org/journal/index.php/ajis/article/view/8958.

18 Ian Walden, Accessing Data in the Cloud: In: Cloud Computing Law, Oxford University Press (2021). DOI: 10.1093/oso/9780198716662.003.0013

19 Holt (n 3) p 94.

20 The distinction between data ‘at rest’ and ‘in transmission’ does not denote the technical state of the data, since data held by a cloud service provider, ie ‘at rest’ may be regularly ‘in transmission’ between internal resources of the service provider, eg using load balancing. Rather the phrases are used to indicate a legal distinction between LEA powers of access to data, See Walden Cloud p 443.

21 Walden (n 18).

22 GeeksforGeeks, Difference between Data and Metadata, https://www.geeksforgeeks.org/difference-between-data-and metadata.

"Warrant-proof" encryption entails that the LEAs are unable to obtain electronic evidence necessary to investigate even if they have a warrant. As quoted by Rosenstein, encrypted communications are "law-free zones that permit criminals and terrorists to operate without detection by police and without accountability by judges and juries"[23]. It is, essentially, a technology that transforms the data you leave in cyberspace, into unintelligible cyphertexts, that need a specific key to be read by the computer. In the case of VPNs, the encryption is done by the Internet Service Provider (ISP), and they can remove it if asked by the law enforcement request to give them encryption[24]. The challenge is that law enforcement agencies lack the tools, techniques and expertise needed to counter the criminal abuse of encryption.[25]

As Europol and Eurojust highlight, in investigations and prosecution of any criminal conduct that happen in real or virtual world, the electronic evidence is expected to replace classical form of evidence used to build a case.[26] As something that can affect criminal proceedings in general in the future, the notion of digital footprint needs to be better regulated in many jurisdictions.

Digital Footprint refers to the traceable data and metadata a user manifests on the internet.[27] Through tiny pieces of information that users willingly leave behind, corporations can send customized adds, and cybercriminals can commit personalized crimes. Nonetheless, despite that there is a plethora of articles on how to protect your data and hide your digital footprint, there is a growing perspective that this type of information can be of help in criminal investigations.

III. Cybercriminal, Cyberidentity, Cyberprofiling - cyber how?

There is an profusion of data and research that reflect how cyberspace affects the real world - for good or bad. For the latter, there has been a necessity

23 Walden

24 Cybercrime Convention Article 19.

25 Joint Report, Europol and Eurojust Public Information, Common Challenges in combating cybercrime, (2019) p 11.

26 ibid p 20.

27 Kaspersky, What is a digital footprint? And how to protect it from hackers, https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint.

to reflect how to deter criminal activity by legislators and policy makers.[28] As the traditional law's application to these new criminal behaviours was often certain, most jurisdictions have adopted sui generis approaches to tackle cybercrime.[29] Perhaps unsurprisingly, the most common approach has been to focus on the cyberspace, the technology and the data, without first giving a thought to the most important element: who commits the crime.

3.1 Who are the cybercriminals?

A cybercriminal is "a person who conducts some form of illegal activity using computers or other digital technology such as the Internet".[30] They exploit the interconnectivity of the internet, the anonymity it offers and easy getaway to commit crimes, either in cyberspace or the real space.[31] Researchers have begun to explore the characteristics of criminals that use technology to commit crime[32], in a nouveau approach from the hacker/tech savvy perpetrator.

Cybercriminals that commit cyber-enabled offences do not need to be knowledgeable in STEM related fields.[33] Essentially, in these particular type of offences, the perpetrator uses the cyberspace in four ways:

- To buy illegal goods, stolen data and information in marketplaces;
- To recruit people to commit crime;
- To sell illegal goods, child pornography or
- To amplify crimes like terrorism.

Cyber-enabled offences function in tandem, combining elements of hacking, anonymity, and cooperation in order to affect large populations.[34] Research has found that people get involved in cybercrime "due to the lack of deterrents, increased anonymity, and repressed desires to offend in the

28 For example, Ian Walden, Computer Crimes and Digital Investigations (2016), 2nd edn, OUP.

29 ibid.

30 John Sammons, Michael Cross, in The Basics of Cyber Safety, 2017, Editor(s): John Sammons, Michael Cross, Pages 87-116,

31 Guide for Good Governance on Cyber Security, DCAF – Geneva Center for Security Sector Governance, Geneva – 2019, Available online: https://dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdfstr

32 ibid

33 Casey, Handbook of Digital Forensics and Investigations (2009), Academic Press.

34 Holt and Bossler (n 4).

real world".[35] It must be concluded therefore that to repel this phenomenon, we need to increase deterrents, decrease anonymity and study more the repressed desired to offend in the real world.

3.2 A new proposal - cyberidentity?

"What is illegal offline should be illegal online" was observed by the European Council of the European Union in a press release in 2021.[36] It is perhaps interesting to ponder on the double standard people have towards cyberspace and the real world. Most of the things that are illegal in the real world, are in fact allowed, or overlooked in cyberspace - an example would be defamation and hate speech. They are both illegal in cyberspace and the real world, but the mechanism of enforcing it in cyberspace falls behind of that of the real world. For the reasons mentioned above, anonymity tools, jurisdiction problems or lack of willingness from the prosecution, leaves room for improvement in many areas.

Intending to rectify the problem of anonymity, authors are researching on how to introduce the notion of Cyber-Identity/digital identity.[37] The recommendation is for users to have a virtual identity, which others may or may not see, but can and will be always disclosed to judicial authorities in case there is suspicion of a crime. This cyber persona will be used for user identification and intent. Biometric identification is another notion that is mirrored by the real world, inflicting a possible future where users in cyberspace will be identified by international agreed rules. Altogether, these measures go in tandem with the ethics of " when a cyber identity has done something wrong, the person behind that identity will be punished."[38]

3.3 Cyberprofiling

In this digital age, data and metadata serve a key component in identifying

35 ibid.

36 European Council of the European Union, What is illegal offline should be illegal online: Council agrees position on the Digital Services Act https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/.

37 See generally Clare Sullivan, Digital Identity: an emergent legal Concept, The University of Adelaide press: For the author, in an online environment being asked to provide 'ID' will become as commonplace as being asked one's name.

38 Cyberethics, What is Right or Wrong in the World Wide Web, http://individual.utoronto.ca/diane_flores/cyberidentity.htm.

crimes and criminals, in cyberspace and in real life. Nonetheless, such data and metadata are meaningless if law enforcement cannot use them in the right time. Cyberprofiling is defined as "an idiographic analysis on a subject's digital footprints so as to reveal information that can help identity or better understand the subject."[39] It reflects the approach to combine criminological techniques of profiling with computer related data[40]. Research anticipates that profiling will help law enforcement agencies to detect and predict methods not only on existent networks, but also in new networks that could be used for illegal purposes.[41]

Criminal Profilers need to train and gather knowledge in the detection of cybercrime-enabled crime as a multi-disciplinary field. In general, there is a lack of comprehensives strategy to identify, stop and punish cybercriminals.[42] As Eoyang notes, it is imperative to rebalance the cybersecurity policies from focusing on better cyber defences against intrusions, to humans.[43] The key elements that the author highlights for policymakers, are (1) identify malicious acts, (2) enhance diplomatic efforts, and (3) develop measurable strategic plan to fight cyber-enabled crime.[44]

IV. Issues and Solutions - What can LEA do?

From the standpoint of criminologists, law enforcement agencies need to continue their ordinary, covert[45], and coercive policing techniques[46]. The legal developments have introduced new rules that that require ISP to retain set of data - not directly a new law enforcement power, but it indirectly says that ISP need to save the data, which ordinarily would have them deleted or destroyed.

---

39 IGI Global, https://www.igi-global.com/dictionary/cyber-profiling-in-criminal-investigation/89687.

40 Eur Ing Brian C. Tompsett, Angus M. Marshall and Natasha C. Semmens, Cyberprofiling: Offender Profiling and Geographic Profiling of Crime on the Internet, (2005) Computer Network Forensics Research Workshop, 1.

41 ibid, p 3.

42 EU cyber security strategy: An open, safe and secure cyberspace, Available online: https://www.cyberwiser.eu/content/eu-cyber-security-strategy-open-safe-and-secure-cyberspace.

43 Mieke Eoyang, To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors (2018) p 4.

44 ibid

45 Covert techniques - lawful interception - listening in to a conversation, see more Ian Walden, Addressing the data problems: cyber- forensics and criminal procedure, p 4.02.

46 Coercive - the ability to stop and search people against their will, see more Ian Walden, Addressing the data problems: cyber- forensics and criminal procedure, p 4.02.

4.1 Data & Metadata - Traffic Data

As was previously stated, the data issue is one of the prominent drawbacks of the law enforcement investigations. Data might be encrypted, lost or in transmission, and as a result, difficult to be used and attained for investigation purposes. In this case, traffic data might be useful to trace the source of a communication in an electronic communication network.[47] The Budapest Convention defines traffic data as any computer data that indicates the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[48] In principle, although traffic information does not include content, it yet can provide sufficient information to work on profiling and leads. From a law enforcement perspective, this kind of data helps to trace and locate geographically and chronologically the end user device that transmitted the initial information.[49]

Another solution might be to design a system that can provide with the capabilities to give law enforcement authorities a backdoor or design a service that permits the data to be there. In the Apple vs FBI case[50], the FBI asked Apple to assist them in decrypting the phone of a person under investigation. Apple refused as it could not breach the security of the phone and bypass the encryption software. Then the FBI found another solution to the encryption problem: Get help from a third party. The question is if the government has the key to the back door, how hard is for someone else to get it? This is because providing a backdoor essentially makes the system less secure

In the UK, Investigative Power Act section 252 provides the Internet Service Provider with the legal capability to build a backdoor and requires ISP to design a service that lets the law enforcement access to the data stored in the servers.[51]

---

47 Caroline Goemans and Jos Dumortier, Enforcement Issues — Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity, 161, p 2.

48 Cybercrime Convention, Article 1/d, http://conventions.coe.int/Treaty/en. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging. See Explanatory Report to the Convention on cyber crime, Council of Europe, 8.11.2001, to be consulted at: http://conventions.coe.int/Treaty/en.

49 Goemans, (n 44) p 6.

50 Apple v FBI

51 IPA (n 15) section 252.

Also, the Data Retention laws[52] specifically requires ISP to keep specific types of data for enforcement purposes. UK law implements this requirement through procedures detailed in Part III of the Regulation of Investigatory Powers Act 2000 (RIPA), 'Investigation of Protected Electronic Information'. Under the RIPA, a person may be served with a notice requiring that he or she need to either disclose the identified information in an 'intelligible form' or provide the 'key' that enables access to the requesting agency. Distinguishing in this sense legitimate from unlawful usage (could it be justification to get the key code?). Nonetheless, establishing a *mens rea* for technologies designed for general application is a very high threshold which might not be met in most of the cases. Cracking cryptography through 'brute force' computational techniques is only likely to be an option for national security agencies, who may have the necessary resource to throw at the problem

Today, the much more likely target of attack is not the encryption itself - it's just the end points. In case that the law enforcement can get access to the computer and device where the data is being transmitted, then they can access the encrypted data – if they bypass the passcode of the suspected. In case this does not work, many raise the question whether there is even a need to discuss on encryption?

4.2 Unique investigative tools

To begin with solutions, the encryption and anonymity problem can be dealt with criminalising the supply, possession or use of technologies that facilitate cyber-enabled crime.[53] Nonetheless, as Walden notes, it is a challenge to distinguish legitimate and unlawful uses of such technology. As a result, LEAs need to resort to other tools and techniques to investigate cyber-enabled crime.

Cybercrime investigations techniques that might help in a cyber-enabled crime are:

- Background check
- Information gathering:
- Tracking and identifying the authors:

52 Data Retention Directive, Directive 2006/24/EC on the retention of data generated in connection with the provision of publicly available electronic communications services or of the public communications networks and amending Directive 2002/58/EC, OJ L 105/54, 2006.

53 Cybercrime Convention, Article 6: Misuse of devices.

- Digital forensics:[54]

There is a plethora of forensics tools that are created to assist LEAs in their examinations, i.e., tools that can be used to examine digital forensic data, analyse disk images and recover files, perform disk cloning and imaging, and access local and remote devices.[55] Nonetheless, gaining access to the plaintext of encrypted messages is expensive and often difficult. A proposal for this would be for enforcement agencies to train on reverse engineering.

- Wiretap the society?

A practice generally followed by US and UK (among other countries) is the monitoring of the domestic communication. Intelligence agencies monitor the traffic and look for patterns that might indicate if a crime is happening. Certainly, these powers are compliant with human rights safeguards and limited in scope.[56] This highlights the importance of braining data related to the suspected offender's activities.[57] Another option would be to (1) gather data from 'open source' intelligence, (2) get data from a CSP, or (3) obtain data coercively through the exercise of search and seizure.[58]

4.3 Training and cyber strategizing

The increased risk of the cyber element in crime, and the novelty of ways to use technology to commit crime, calls for increasing capacities for LEAs. Cyber crime investigators need better cyber forensic capabilities and trainings[59]. In the National Initiatives for Cybersecurity Careers and Studies in the US, the cybercrime training for Law Enforcement aims to educated officers on "on how to think like hackers as well as how to identify the tools that hackers use to commit attacks".[60] Researchers call for a transformation on the way cyber-related professionals are trained, incentivized, and retained

54 SecurityTraills, Cyber Crime Investigation Tools and Techniques Explained, https://securitytrails.com/blog/cyber-crime-investigation.

55 ibid.

56 Lewis, James A., Denise E. Zheng, and William A. Carter. "Front Matter." The Effect of Encryption on Lawful Access to Communications and Data. Center for Strategic and International Studies (CSIS), 2017. http://www.jstor.org/stable/resrep23146.1., 24

57 Walden, Addressing the data problem, p 4.05.

59 Eoyang (n 40).

60 Cyber Crime Training For Law Enforcement, https://niccs.cisa.gov/education-training/catalog/national-cyber-security-university/cyber-crime-training-law-enforcement.

so they can be more productive in catching cybercriminals.[61]

Furthermore, drafting an effective cyber strategy in national level can help the organization, LEAs in this instance, to understand and address how data, networks, technical systems, and people.[62] An informed plan of action that will prepare officers to deal with cyber-enabled crimes is a desired solution that might bring positive outcomes.

In a report on cybersecurity maturity level in Albania, it was noted that the criminal justice system was working towards a better cybercrime strategy. Nonetheless, the cybercrime unit remain understaffed, with a lack of resources to fully investigate a cyber-enabled crime. For this reason, the research recommended to strengthen national investigation capacity, increasing human and technologic resources, and establish operational cybercrime units at a local level.[63]

4.4 International Cooperation

Cybercrimes transcend borders, leave evidence in many territories, and put into question the notion of jurisdiction. Hence, law enforcement agencies need powers to acquire data, which may be stored, controlled, operated in another country. Judicially mutual assistance is the cooperation between criminal authorities, prosecution, or judicial authorities.

For instance, Mutual Legal Assistance is the cooperation between criminal authorities, prosecution, or judicial authorities.[64] When the state needs to carry out criminal investigations outside its jurisdiction and need to corporate with the state where the information is stored and/or controlled, then they need to request legal assistance from that country. The Second Protocol to the Cybercrime Convention builds upon the gaps of MLA, and states have an international obligation to corporate, as it is not on ad hoc basis or on the good will of the states to cooperate. Second Additional Protocol prescribes an expedited form of co-operation for subscriber information[65]

61 Eoyang (n 40).

62 Yuri Diogenes, Cybersecurity: Attack and Defense Strategies (2018), p 39.

63 The review was conducted in cooperation with the World Bank and the dissemination of this report was carried out in cooperation with Global Cybersecurity Center for Development (GCCD) under Korea Internet Security Agency (KISA) of Republic of Korea. The financing came from the Korea --World Bank Group Partnership Facility (KWPF), which is administered by the World Bank for Korea's Ministry of Strategy and Finance

64 European Convention on Mutual Assistance in Criminal Matters 19959 - EU (200)

65 Cybercrime Convention (n 4) Art 18(3): 'means any information, contained in the form of

and traffic data, around 20 days for subscriber information and 45 days for traffic data. In emergency situations ("life & limb"), the procedure might be expedited.

Another mechanism for international cooperation is the UK-US agreement. When UK makes a request to the US to get data about a crime that leaves traces in the cyberspace, US makes the international request part of the domestic jurisdiction - and supplies the information. Similarly,

European Investigation Order (EU judicial mechanism)[66] even though it does not investigate the request, it treats it in a non-discriminatory way. For example, UK sends a request to France, so France will make it a 'French order' on its standards, but it will treat that UK order as if it is an UK order (treat it in a non-discriminatory manner) - therefore it will process the request. With the European Preservation Order, the recipient country highlights that they trust the law that exists in the UK to be the same as the law that exists in France, and therefore they do not have to tell the recipient country and can go straight to the Internet Service Provider – this is essentially an acceptance of foreign law or a surrender of sovereignty, and is the same analogy that follows the U.S.-U.K. Agreement to Access Electronic Data for the Purpose of Countering Serious Crime. Essentially, not discriminating the request and extending the powers of the foreign law enforcement to reach Internet Service Provider directly, without approving and formalising such request, would be the missing improvement that might be reflected on a bilateral agreement.

In my opinion, such an option is worth considering on how to go beyond the Cybercrime Convention. Cross-border offences translate in more people acting against the law, more victims, and damages. There is a necessity for international cooperation in the investigation of organised crime, drug, and human trafficking cases, collaborate on preservation and recovery of intelligence, and enforce criminal law.

---

computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:
a. the type of the communication service used, the technical provisions taken thereto and the period of service.
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing, and payment information, available on the basis of the service agreement or arrangement.
c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.'

66 European Investigation Order Directive 2014/41/EC

4.5 Use the cloud

The cloud refers to the technology that makes possible for consumers, businesses, and governments, to store their data in data centres using cloud computing technology. Another group that has taken an interest upon cloud services are cybercriminals - who use cloud services as a tool to commit crime or as a target.[67] For this reason, as Walden argues, law enforcement agencies might consider accessing obtaining access to data held in the cloud services for forensic purposes.[68]

Despite the jurisdictional debate that accessing the cloud enacts (that falls outside the scope of this paper), it is important to highlight that the legal developments in this have been positive towards a potential reach of law enforcement agencies to data in the cloud.[69] For instance, the Cloud Act[70] does not provide for bulk disclosure of data, but it needs to identify "a specific person, account, address, or personal device, or any other specific identifier" and it needs to be necessary and subject to judicial oversight or review.[71] Similarly, The European Public Prosecutor's Office (EPPO) will grant capabilities to LEAs to request access to users' content, traffic data, and subscriber data regardless of the location and data.[72]

Exploring how to extend the investigative powers to the cloud, whilst complying with the human rights safeguards, would prove to be an important step to identify a suspect of a criminal activity. Nonetheless, it is important to note that establishing an adequate forensic link between the data in the cloud, the user from which the data was pin-pointed, and the individual users is a complex and hard task.[73]

V. Conclusion

"As the world moves into a hyper-connected society with universal internet access, it is hard to imagine a 'computer crime', and perhaps any crime, that

67 Ian Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (2021), p 441.

68 ibid

69 Council of Europe, Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' T-CY (2016) 5 https://www.coe.int/ en/web/cybercrime/ceg.

70 UK–US Bilateral Agreement (Art 1(3).

71 Walden (n 63), p 441

72 Walden (n 63, p 463 citing eEvidence proposal (n 88) Art 1(1).

73 Walden (n 63),

will not involve electronic evidence linked with internet connectivity."[74]

In conclusion, establishing a link between data, the virtual identify and the real persona - for forensic procedures, is not an easy task. The identity problem proves to be complex in cyber-enabled crimes in particular, as the data traces are connected mainly with acquiring the means to commit the crime in the real world and not with the consequence or connecting the dots between the author of the crime to the offence. Nevertheless, there is an improvement towards understanding data and how to use them in this conundrum. Options that are recommended in this paper are cyberprofiling, as a mean to create profiles of risks in the society, or even pushing forward the agenda on the legal notion of Digital identity.

The problem of encryption is not reflected as problem per se in this paper. The government continues to argue that it needs access to messages to investigate criminals and terrorist, but tech companies are set in the position that it might bring a potential violation of privacy. Whereas criminologists are reluctant to go to either camp and are set with exploring innovative ways to investigate crime offenders by the use of traffic data, metadata and subscriber data.

This paper draws on the importance to focus on catching the human attacker, building up law enforcement, enhancing international cooperation and developing a measurable strategic plan to counter crime both in the cyber and the real world. All things considered, identity in cyberspace is anticipated to be regulated in the following years. As there is a shift on the thought process of the policymakers for what is allowed, criminalized, and enforced in the cyberspace, such debates on anonymity and hidden persona, might get new redirections.

What is illegal offline should be illegal online.

Bibliography

Bada, Maria and Hameed, Faisal, Report on Cybersecurity Maturity Level in Albania (January 15, 2019). Available at SSRN: https://ssrn.com/abstract=3658345.

Clough, J., Principles of Cybercrime. 2nd Edt. Cambridge Press (2015).

Diogenes Y, Cybersecurity: Attack and Defense Strategies (2018).

74 United Nations Office on Drugs and Crime (UNODC), Draft Comprehensive Study on Cybercrime, (2013).

European Commission: "Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace", (dated on February 7th 2013) available online: https://data.consilium.europa.eu/doc/document/ST%20 6225%202013%20INIT/EN/pdf.

Goemans C and Dumortier J, Enforcement Issues — Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity, 161.

Holt TJ and Bossler AM, An Assessment of the Current State of Cybercrime Scholarship (2014) 35 Deviant Behavior 20.

Krueger, C., McKeown, S.: Using Amazon Alexa APIs as evidence, IEEE International Conference on Cyber Incident Response, Coordination, Containment & Control, (2020).

Shkembi, A., Shtupi, I., & Qafa, A. (2016). The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation. Academic Journal of Interdisciplinary Studies, 5(1), 127. Retrieved from https://www.richtmann.org/journal/index.php/ajis/article/view/8958.

Walden I, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (2021).

Walden, I., Addressing the data problems: cyber forensics and criminal procedure.

Walden, I.,'The Sky is Falling!' – Responses to the 'Going Dark' problem, computer law & security review 34 (2018) 901–907.

Legislation

Council of Europe Convention on Cybercrime, ETS No 185 (Brussels, 23 November 2001, entered in force 1 July 2004).

UK, Investigatory Powers Act 2016

Use of Data Act, enacted as part of the Consolidated Appropriations Act, 2018 (CLOUD Act).

Data Retention Directive, Directive 2006/24/EC.

Nr. 9918 law, date 19.05.2008 "On electronic communication in the Republic of Albania"

Nr. 9880 law, date 10.03.2008 "On protection of personal data"

THE LIE DETECTOR THAT LIES?
POLYGRAPH TEST IN THE EMPLOYMENT RELATIONSHIP OF PUBLIC SECURITY EMPLOYEES.

MSC. ARTEMIDA HOXHAJ

Attorney at law at "Lawyers & More" law firm

External lecturer on the subject of "Constitutional Law"

Faculty of Law – University of Tirana

artemidahoxhaj@hotmail.com

Abstract

The polygraph is an instrument that measures and records certain physiological data of a subject under controlled conditions in an attempt to detect deception, based on the theory that an individual exhibits certain predictable physiological characteristics every time that he intentionally tells a lie.

In recent years, the use of the polygraph in the workplace, especially for public security employees has increased significantly, in some countries even to the point where the number of polygraph tests as a criterion for employment or as an evaluation criterion in the employment relationship is greater than the number of tests performed for the purposes of criminal proceedings. This has been accompanied by growing concern not only about its accuracy but also the implication of the violation of a number of human rights such as human dignity, the right to private and family life, the right to employment, etc.

Therefore, this paper focuses on the use of the polygraph test, known more commonly as the "lie detector," in the employment relationship of public security employees. Paying special attention to the legal and judicial provisions for its use in the Republic of Albania as a criterion for the selection of the head of the National Bureau of Investigation and investigators of this institution, as well as as a criterion for evaluating the employees of the State Police, Guard of the Republic and the Service for Internal Affairs and Complaints in the Ministry of Interior, but not leaving aside the comparative approach with other states.

Keywords: polygraph test, lie detector, human rights, public security, workplace

Introduction

Since the beginning of time man has been looking for an efficient way to flush out the lie. Various innovative techniques were tried. Some were ridiculous, others cruel, but they were all based on the assumption that some physiological reaction occurred when a person was confronted with a specific event under investigation and that this reaction would have a detectable external manifestation.[1]

It is impossible to pinpoint when people first began noticing the relationship between lying and observable changes in the body. The early Greeks founded the science of physiognomy in which they correlated facial expressions and physical gestures to impute various personality characteristics. The ancient Asians noted the connection between lying and saliva concluding that liars have a difficult time chewing and swallowing rice when being deceptive. Clearly, behavioral detection of deception pre-dates instrumental detection of deception which, it is equally clear, is European in origin.[2]

In 1730, the British novelist Daniel Defoe in his essay "An Effectual Scheme to the Immediate Preventing and Suppressing of Street Robberies all Other Disorders of the Night" advanced a theory that the pulse of a suspicious person can reveal that the person is lying. In 1878 the Italian physiologist Angelo Mosso used an instrument called a plethysmograph to

1 Brief history of the polygraph, Norman Kelly Polygraph Expert, http://www.kellypolygraphe.com/polygraph-history.php accessed June 16, 2022.

2 Chicago: Where Polygraph Becomes a Science, Stanley M. Slowik, Frank S. Horvath, EUROPEAN Polygraph, Volume 13, 2019, Number 1 (47).

detect the change in blood pressure in response to certain stimuli. Meanwhile, Sir James Mackenzie, MD, constructed the first polygraph in 1892. An instrument that could be used during medical examinations with the ability to simultaneously record undulated traces of vascular pulse (radial, venous and arterial), by way of a stylus on a rotary drum of smoked paper.[3]

The first use of a scientific instrument to measure physiological responses was in 1895 when the doctor, psychiatrist, and Italian criminologist Cesare Lombroso, modified an existing instrument called a hydrosphygmograph and used it to measure physiological changes in the blood pressure and pulse of a suspect questioned by police [4]

Lombroso would fit a rubber glove to a tank of water and insert the suspect's hand. Changes in the water's height were thought to correspond to changes in the hand's blood volume while lying.[5]

At Harvard University's Departments of Psychology and Physiology, William James, Walter Cannon, Hugo Münsterberg, and his student, William Moulton Marston, all conducted significant work in psychological theory relevant to the present-day polygraph. William James was the first to define emotions as bodily changes, specifically, that such changes were responses to recognizing an exciting stimuli. This notion was later captured in the somewhat simplistic *"Fear does not make us run from the bear – running from the bear makes us experience the emotion of fear"*. [6]

Ever since the dawn of the modern-day polygraph, the test has spawned both innumerous cultural references and polarizing critiques. While the most common concern is about the test's accuracy, other concerns include fears about juror abdication (the role of the juror becoming co-opted by machines) as well as concerns about civil rights infringements. Searching for a definition of a polygraph is in and of itself indicative of some of these concerns. For example, even describing the polygraph as a "lie detection test" is subject to criticism. Some find it more accurately described as a "fear detector" or, more generally, an emotion detecting test.[7]

---

3 Brief history of the polygraph, Norman Kelly Polygraph Expert, http://www.kellypolygraphe.com/polygraph-history.php accessed June 16, 2022.

4 Brief history of the polygraph, Norman Kelly Polygraph Expert, http://www.kellypolygraphe.com/polygraph-history.php accessed June 16, 2022.

5 An "Unfair and Cruel Weapon": Consequences of Modern-Day Polygraph Use in Federal Pre-Employment Screening, Ariela Rutbeck-Goldman, IC Irvine Law Review, Vol. 7:715.

6 Chicago: Where Polygraph Becomes a Science, Stanley M. Slowik, Frank S. Horvath, EUROPEAN Polygraph, Volume 13, 2019, Number 1 (47).

7 An "Unfair and Cruel Weapon": Consequences of Modern-Day Polygraph Use in Federal Pre-

There are different approaches in different countries, such as regarding the use of this test as evidence in criminal proceedings (generally prohibited to a large extent), as well as in proceedings of an administrative nature, such as in employment relations in various positions of which are related to public security.

In relation to the latter, from a jurisprudential point of view, it is estimated that the polygraph test means an apparatus that continuously and simultaneously records both cardiovascular, respiratory, and electrodermal data. The test results can serve as data to determine the integrity of the person undergoing the procedure, based on the truthfulness of his answers. It is applied in labor relations only for certain public structures, which require in their ranks employees of high integrity.[8]

Polygraph testing in the workplace is said to be highly contentious and controversial, as the admissibility and reliability of its results remain unclear. However, polygraphists have been accepted as expert witnesses whose evidence needs to be tested for reliability. Polygraphists are usually called to testify on how the test was administered, his/her qualifications, the type of test used, and the questions asked.[9]

A comparative overview of the use of the polygraph test in employment relations

In the USA, the polygraph test is one of the tests that must be completed by the individual seeking employment in certain public institutions. The Justice Department continues to agree with the House Government Operations Committee's conclusion that "the polygraph machine is not a ``lie detector,'' nor does the operator who interprets the graphs detect "lies". The tool records physical responses, which may or may not be related to an emotional response, and the response is not necessarily related to guilt or innocence. Many physical and psychological factors make it possible for an individual to defeat the polygraph by avoiding the machine's discovery of the truth.[10]

Employment Screening, Ariela Rutbeck-Goldman, IC Irvine Law Review, Vol. 7:715.

8 An "Unfair and Cruel Weapon": Consequences of Modern-Day Polygraph Use in Federal Pre-Employment Screening, Ariela Rutbeck-Goldman, IC Irvine Law Review, Vol. 7:715.

9 Deceptive or effective? Polygraph testing in the workplace, Hogan Lovells, April 2014, https://www.hoganlovells.com/en/pdfdownload?page={AAE4CB5E-B764-4356-AD8C-7876BBF70F1A}&p=1, accessed 11 June 2022

10 Employee Polygraph Protection Act of 1988, Pub. L. 100-347, Sec. 1, 29 U.S.C. §§ 2001 et seq.

Meanwhile referred to the Employee Polygraph Protection Act of 1988 (EPPA) which is a United States federal law that generally prohibits most private employers from using lie detector tests either for pre-employment screening or during the course of employment, with certain exemptions, employers are generally prohibited from requiring or requesting any employee or job applicant to take a lie detector test, and from discharging, disciplining, or discriminating against an employee or prospective employee for refusing to take a test or for exercising other rights under the Act.

Federal, State, and local governments are not affected by the law. Also, the law does not apply to tests given by the Federal Government to certain private individuals engaged in national security-related activities. The Act permits polygraph (a kind of lie detector) tests to be administered in the private sector, subject to restrictions, to certain prospective employees of security service firms (armored car, alarm, and guard), and of pharmaceutical manufacturers, distributors, and dispensers. The Act also permits polygraph testing, subject to restrictions, of certain employees of private firms who are reasonably suspected of involvement in a workplace incident (theft, embezzlement, etc.) that resulted in economic loss to the employer. The law does not preempt any provision of any State or local law or any collective bargaining agreement which is more restrictive with respect to lie detector tests.

Where polygraph tests are permitted, they are subject to numerous strict standards concerning the conduct and length of the test. Examinees have a number of specific rights, including the right to a written notice before testing, the right to refuse or discontinue a test, and the right not to have test results disclosed to unauthorized persons.

In terms of its elaboration in jurisprudence, the Los Angeles Supreme Court[11] considered the request of the police association of this city, which claimed that the procedures for promotion, parallel movement, or appointment to job positions for which submission to the polygraph test was also required, it was an unfair legal provision and had to be canceled. In this case, the court stated that persons who express their willingness to be appointed to sensitive duties must undergo a polygraph test, as such jobs require the "highest level of integrity". Such duties included working in anti-terrorist, anti-narcotics, and organized crime activities.

Even in the case of Oberg v. City of Billings, December 22, 1983 (see

Section 2001(3), enacted by the US Congress

11 Los Angeles Police Protective League v. City of Los Angeles, 1995

paragraph 41 of this decision), the Montana Supreme Court on the polygraph test stated: *"Legislators were concerned about the types of questions that could be used by polygraph examiners creating a response model and this concern was expressed in the committee hearings that preceded the adoption of this law. We cannot assume that when administering a polygraph test, all questions will be limited to employment-related matters only. Assuming, moreover, that the statute was enacted specifically to exempt police officers from the general statutory protection afforded to all other employees in this state, we doubt that such an exemption would "survive" a strict examination".*

In Europe, the polygraph test is provided in some countries.

In Lithuania, the law "On the use of the polygraph", dated August 29, 2000, defines, among other things, the list of institutions that can apply the polygraph test, namely: Police Department, State Security Department, Border Protection Service, the agencies of the Ministry of Internal Affairs, the Department of Operational Services under the Ministry of Defense of the Region, the Customs Department of the Ministry of Finance and the Special Investigation Service. The law prohibits the use of the polygraph by other institutions, but they can perform it: 1) in cases where they are allowed access to information that constitutes a state secret and in relation to persons suspected of having provided false biographical information; 2) for the process of investigating criminal offenses committed during service in internal investigations, as well as in special investigations; 3) in cases of committing crimes and other illegal actions, as well as in cases of violation of the work regime when the information constitutes a state secret; 4) in cases of suspicion of exerting pressure on the person who has access to information that constitutes a state secret; 5) in the case when the tested person requests repeated testing on his own initiative. According to the law, the polygraph is applied to the testing of civil servants, officials, military personnel of the mentioned institutions.

In Poland, the polygraph test is used for recruiting personnel of law enforcement institutions (Police, Military Intelligence Service, Military Counterintelligence Service, Customs Bureau, Internal Security Agency, Intelligence Agency, Central Anticorruption Bureau and Border Guard Service). The legal basis is the internal regulation of these institutions. The test cannot contain questions about internal or religious beliefs. If the test results are inconclusive, then they can be repeated only once, within 30 days of the first interview.

Regarding the importance that the polygraph test should have in the recruitment of employees, the Constitutional Court of Moldova has emphasized that *"the condition to pass the polygraph test should be only a matter of procedure and not essential"*.[12]

The case of Albania

In Albania, the polygraph test, according to law no. 95/2016 "On the organization and functioning of the institutions to fight corruption and organized crime", is provided for candidates for director and investigator of a special structure, such as the National Bureau of Investigation (hereinafter NBI), which is a body constitutional under the Special Prosecutor's Office Against Corruption and Organized Crime (hereinafter SPO), with competence to investigate criminal offenses of corruption and organized crime. The director of the NBI is responsible for its operation. The director, deputy director, NBI investigators, and officers of the Judicial Police in the exercise of their functions are directed and controlled by special prosecutors. NBI employees maintain the secrecy of criminal investigations, in accordance with the Code of Criminal Procedure and legislation in force (Article 40 of Law No. 95/2016). NBI is the institution that executes wiretapping orders requested by the Special Prosecutor's Office and authorized by courts against corruption and organized crime.

The legislator in the law no. 95/2016, among other things, had the purpose of guaranteeing the functioning of the NBI to investigate criminal offenses of corruption and organized crime, as well as other criminal offenses committed by the entities provided for in Article 135, point 2, of the Constitution, independent of any illegal influence, internal or external. This need has been dictated due to the size and level of spread of the corruption phenomenon in Albania, which has also affected the effective functioning of the rule of law.

The Constitutional Court of Albania, with decision no. 20, dated April 20, 2021, estimated that the spread of corruption has brought the need for the establishment of special bodies to fight it and at the same time, to strengthen the integrity and trust of the public in their functioning, it affects the taking of appropriate measures that in these institutions employ persons with high moral values. These measures necessarily included the NBI, as a unit whose function is to investigate criminal offenses against corruption and organized crime.

12 Decision no. 6 dated April 10, 2018 of the Constitutional Court of Moldova

For the above, the Constitutional Court assesses that the legislator by subjecting the candidate to the polygraph test, during the employment procedures at the NBI institution, according to law no. 95/2016, there is a public interest, which justifies the intervention. The public interest, in this case, is related to the fight against corruption, as well as taking measures, and creating special institutions in the composition of which people with moral qualities and high professional skills should be employed.

Regarding the results of the polygraph test, the Constitutional Court considers that they do not constitute a disqualifying criterion in the procedure for appointing candidates for director and investigator of the NBI, but must be evaluated by the Special Commission together with the verifications for the control of assets and the purity of the candidate's image, as also resulted from the explanations of the interested entity, Special Structure Against Corruption and Organized Crime, for the current practice of implementing the law in question, according to which only the results of the polygraph test were not used as a disqualifying criterion during the appointment procedure of the NBI director and investigators. Consequently, in the assessment of the Constitutional Court, only failure to successfully pass the polygraph test, in cases where the criteria for property assessment and image control have been met by the candidates, cannot constitute a disqualification criterion in the process of appointment for director and investigator of the NBI.

Also, the Constitutional Court notes that the information obtained from the results of the polygraph test is included in the concept of "data collected about the individual" and therefore, in this case, all the constitutional guarantees for personal data provided by Article 35 of the Constitution apply, including the prohibition without consent of their publication and the candidate's right to be acquainted with them. Exceptional cases from the constitutional guarantees of Article 35 of the Constitution include only specific situations and according to rigorous procedures, expressly provided by law, such as those that make law no. 8457, dated 11.02.1999 "On information classified as "state secret", amended (law no. 8457/1999).

The Constitutional Court assesses that the results of the polygraph test, in no case, have the value of evidence in the process of appointing the director and investigators of the NBI. The polygraph test is an employment criterion that must be fulfilled by the candidate, and its results are in function of assessing the credibility of this figure.

The Constitutional Court, based on the fact that the legal provisions of articles 34, point 2, letter "gj" and 38, point 2, letter "e", of law no. 95/2016 is

aimed at employing people with moral qualities and high professional skills in the structures whose mission is the fight against corruption and organized crime assesses that the polygraph test in order to justify its purpose, should be implemented in a way well defined. Specifically, failure to consent to the polygraph test disqualifies the candidate, the questions addressed to the latter must be structured to remain within the scope of the law, while the test results, by themselves, have no determining value in the process of appointing the director or investigators of the BKH, in the case of fulfillment by the candidates of other criteria of control of wealth and purity of image.

The polygraph test cannot have determinative value for the results of the appointment process of the NBI director and investigator. Its purpose can be justified only if the process of checking the image and verifying the candidate's assets are not sufficient to complete the full control of his person.

Controversy over polygraph testing validity

"Polygraph" is a term used to describe a device that simultaneously measures and records physiological activities or electro-physiological activity. This data includes an individual's blood pressure, heart rate, respiration rate, and skin conductance (perspiration). The device is essentially utilized to record a person's body reacting to the fear of being caught lying.[13] The polygraph test measures and records physiological responses such as heart rate, blood pressure, breathing patterns, and galvanic skin response while a person is asked and responds to specific questions. Testing consists of taking physiological measurements, interpreting the results, and offering an opinion by a professional polygraph examiner regarding deception.[14]

A polygraph is designed to measure physiological responses. First, the examiner hooks you up to a series of respiratory tubes, leg and arm monitors, a blood pressure cuff, and a fingertip sweat detector. Then, a record is made of your baseline vital signs by asking common questions designed to measure truth: "Are you human?" "Have you ever lied to someone?" (It's assumed that we have all told white lies in our lives.) [15]

13 Deceptive or effective? Polygraph testing in the workplace, Hogan Lovells, April 2014, https://www.hoganlovells.com/en/pdfdownload?page={AAE4CB5E-B764-4356-AD8C-7876BBF70F1A}&p=1, accessed 11 June 2022

14 : Polygraph for Sex Offender Management (Probation and Supervised Release Conditions) | United States Courts, https://www.uscourts.gov/services-forms/polygraph-sex-offender-management-probation-supervised-release-conditions, accesed June 6, 2022

15 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20

Then the real questions begin, with enough repetition and variety to try to catch you in a falsehood. Each question, examiners say, can then be measured against the baseline to see whether it's a lie. [16]

The theory behind polygraph testing is based on the assumption that physiological activity in the human body increases when a person is lying and the polygraph is used to detect that deception. Studies show that when we deceive another person, the part of the brain that regulates emotion, called the amygdala, lights up. We get nervous.[17] Though we think we might be hiding that response from the person we are lying to, inside, our bodies could betray us. Our breathing might change; our heartbeat and blood pressure could rise; our legs or arms could twitch. We might even start to sweat.[18] When we lie *(i.e., deliberately utter a falsehood with the intention to deceive)*, our brain arousal level is increased because of a catecholaminic response that is triggered by the Autonomic Nervous System. This system is also responsible for other body changes that can be detected easily by lie detector tests, including voice modulation, which can be detected via "voice stress analyzers"; pupil mydriasis; increases in respiratory and cardiac frequency; and skin conductance changes (electrodermal response). However, these physiological indexes reflect an emotional perturbation rather than the cognitive act of lying. Therefore, these indexes cannot be used reliably to identify deception if an innocent suspect experiences these physiological changes due to fear. Little is known about the effects of emotional processes (such as the fear of being found guilty despite being innocent) on the physiological responses that are used to detect lies.[19]

---

show%20that%20when%20we,our%20bodies%20could%20betray%20us.
accessed June 8, 2022

16 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us.
accessed June 8, 2022

17 Can you catch a liar? How negative emotions affect brain responses when lying or telling the truth, Alice Mado Proverbio, Maria Elide Vanutelli, and Roberta Adorni, //efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607607/pdf/pone.0059383.pdf, March 25, 2013, accessed June 8, 2022

18 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us. accessed June 8, 2022

19 Can you catch a liar? How negative emotions affect brain responses when lying or telling the truth, Alice Mado Proverbio, Maria Elide Vanutelli, and Roberta Adorni, //efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607607/pdf/pone.0059383.pdf, March 25, 2013, accessed June 8, 2022

The US National Polygraph Association says that *"scientific evidence supports the validity of polygraph examinations"* as long as they are conducted and interpreted with validated procedures. The association points to a meta-analysis of all peer-reviewed studies on polygraph testing that found an accuracy rate of 87%.[20]

The validity of a polygraph reading has been widely criticized. One problem, critics say, is the tendency of humans to lie. The research "Social and Cognitive Correlates of Children's Lying Behavior"[21] shows that children begin fibbing before age 3, and they can master a white lie by age 6, which is also the age most children are busy telling whoppers. [22]

As we grow, some of us become habitual liars, and that can affect how we respond to a polygraph. The study "The brain adapts to dishonesty"[23] published on journal Nature Neuroscience found that as a person lies more and more, the brain becomes desensitized, and is less likely to trigger an autonomic response. Lead study author and neuroscience researcher Neil Garrett said in a statement that *"it is likely the brain's blunted response to repeated acts of dishonesty reflects a reduced emotional response to these acts"*. [24]

Also, the American Psychological Association believes lie detectors are

---

20 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us. accessed June 8, 2022

21 Social and Cognitive Correlates of Children's Lying Behavior, Victoria Talwar, Kan Lee, October 30, 2012, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3483871/pdf/nihms406801.pdf , accessed 9 June 2022.

22 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us. accessed June 8, 2022

23 The brain adapts to dishonesty, Neil Garrett, Stephanie C Lazzaro, Dan Ariely & Tali Sharot, Nature Neuroscience,, Volume 19, No.12, 2016, https://www.nature.com/articles/nn.4426.epdf?sharing_token=N4hMPnUJRQANqOZ2AegfXdRgN0jAjWel9jnR3ZoTv0O2GvX_O5gpKH6ziV8qw4g1x7Bg5UlH_Y7yPXvpGhhKaoKSOZ-qZ9QoyWJ49-xlq9eWiJKBJAK3BCbIFpMrX8Rm0OaC8GMVrbS4jFhj2eHqcZtVKj7oKeeDU3UqViCa1HLJblcjQo3DgjBoCjn1FhmMVD75eNzQNXhyeymg3Ihnj7yjq8kzGNoD6HWQxsf0qFxLJnzR2zcXnmAFV139slRCdbuSy_1IRx0XYtvdqj-Q1Q%3D%3D&tracking_referrer=edition.cnn.com, accessed June 8, 2022

24 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us. accessed June 8, 2022

inaccurate. They say the underlying problem is theoretical: There could be many other reasons for a person to breathe more rapidly or experience a rise in blood pressure, heart rate, and sweat. For example, says the Association, *"an honest person may be nervous when answering truthfully and a dishonest person may be non-anxious"*. [25]

The credibility of the polygraph was challenged almost as soon as it was invented and there is much debate about its accuracy. Some experts say the fundamental premise is flawed.

"It does not measure deception, which is the core problem," says Prof Aldert Vrij, who has written extensively on the subject. "The idea is that liars will show increased arousal when answering the key questions, whereas truth tellers will not. But there is no sound theory to back this up." [26]

Dr van der Zee says that, because taking a lie detector test can be a stressful experience, it can sometimes present innocent people as guilty. "People being interviewed with a polygraph are likely to feel stressed. So whilst the polygraph is quite good at identifying lies, it is not very good at identifying truths," she says. [27]

But Prof Grubin says there are a number of different reasons why a test may be inaccurate. These include the questions being poorly formulated and the interviewer misreading the results. If the examiner is well-trained, if the test is properly carried out, and if there are proper quality controls, the accuracy is estimated between 80%-90%," he says, adding that this is higher than the average person's ability to tell if someone is lying. However, he says that interviewing victims presents a separate problem. Testing victims is a whole different ball game because of the nature of what they're being asked about, you would expect a lot of arousals anyway. This means a victim, especially one recounting a traumatic experience, may appear as if they are lying because they are in an emotional state.[28]

It's difficult to definitively assess how well lie detectors work because

25 The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018, https://edition.cnn.com/2018/03/21/health/lie-detector-facts-accuracy/index.html#:~:text=Studies%20show%20that%20when%20we,our%20bodies%20could%20betray%20us.
accessed June 8, 2022

26 How credible are lie detector tests?, Gareth Evans, October 4, 2018, BBC News https://www.bbc.com/news/world-us-canada-45736631, accessed June 20, 2022

27 How credible are lie detector tests?, Gareth Evans, October 4, 2018, BBC News https://www.bbc.com/news/world-us-canada-45736631, accessed June 20, 2022

28 How credible are lie detector tests?, Gareth Evans, October 4, 2018, BBC News https://www.bbc.com/news/world-us-canada-45736631, accessed June 20, 2022

there are many definitions of deception and many ways of measuring the results, including those deemed "inconclusive." A skeptical 2003 report from the National Academy of Sciences found that polygraphs work at rates well above chance, though far below perfection. "Almost a century of research in scientific psychology and physiology provides little basis for the expectation that a polygraph test could have extremely high accuracy," the report said.[29]

Other factors affecting polygraph examination validity

The premise is that people behave differently, and predictably when they lie. But that's not necessarily the case. The polygraph measures autonomic responses, "and that is all it is measuring," Littlefield said. "Everything else is interpretation. If you want to look at a record and say, the blood pressure increases when asked this question, that could be for multiple reasons. There are a lot of reasons why your levels and physiology go up and down." These include hypoglycemia, fear, confusion, PTSD, nervousness, alcohol withdrawal, psychosis, and general anxiety. Tellingly, in her own experiment, Littlefield found that a person's body can trigger similar test results when undergoing "stressful truth-telling" as when lying.[30]

According to a Technical Memorandum of the U.S. Congress, Office of Technology Assessment, there are some other factors that can affect polygraph examination validity, e.g.:

The examiner's skill

The examiner's skill has an important effect on the validity of polygraph tests. Examiner experience is an essential element reported by investigators and has often been used to explain differences in accuracy rates. There are some data to indicate that experienced examiners have better accuracy rates. In recognition of this outcome, training has been accorded a high priority both within and outside Government agencies which conduct polygraph examinations and by polygraph examiner groups. An extensive array of training facilities now exists, offering a somewhat diverse set of orientations

29 Inconclusive: The truth about lie detector tests, Jennifer Vogel and Madeleine Baran, September 20, 2016, https://www.apmreports.org/story/2016/09/20/inconclusive-lie-detector-tests, accessed June 13, 2022

30 Inconclusive: The truth about lie detector tests, Jennifer Vogel and Madeleine Baran, September 20, 2016, https://www.apmreports.org/story/2016/09/20/inconclusive-lie-detector-tests, accessed June 13, 2022

to polygraph testing. [31]

Subjects

Much effort in recent years has been devoted to development of systematic training. Less attention appears to have been paid to the characteristics of subjects of polygraph testing (e.g.gender, intelligence, existence of other psychopathology, ethnic and group differences, autonomic lability, etc). [32]

Frequently, research reports of polygraph examination do not report even the most easily available data on subject characteristics. Subject factors are often described in the literature as personality or individual difference factors. They refer to traits associated with individuals that may make them differentially detectable in a polygraph examination. Understanding these effects should enable determination of the conditions under which polygraph testing will yield particular levels of validity. The mechanism by which subject variables affect polygraph examination validity has to do with differential autonomic arousal. Validity is affected when an interaction results between arousal and polygraph testing. [33]

Setting

One theory underlying lie detection using the polygraph is that the threat of punishment leads an individual to manifest a physiological reaction. This suggests, then, that settings in which an individual is more certain of being detected and in which the consequences are greatest, will permit higher levels of detection. Furthermore, in order to be certain of being detected, a subject must believe in the efficacy of the polygraph procedures in order for it to function. According to some, the polygraph is often used somewhat

31 Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983, https://sgp.fas.org/othergov/polygraph/ota/index.html, accessed June 15, 2022

32 Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983, https://sgp.fas.org/othergov/polygraph/ota/index.html, accessed June 15, 2022

33 Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983, https://sgp.fas.org/othergov/polygraph/ota/index.html, accessed June 15, 2022

like a "stage prop," and its presence is meant to "enhance the subject's concern." Stimulation tests, used in almost all field polygraph examinations, serve the same function, albeit more directly. There is considerable discussion in the literature about how frequently within a polygraph examination such stimulation tests should be utilized in order to increase the validity of the examination. [34]

Countermeasures

Countermeasures are deliberate techniques used by deceptive subjects to avoid detection during a polygraph examination. Countermeasures can range from simple physical techniques to so-called mental countermeasures, to the use of drugs and biofeedback techniques.[35]

Implications related to basic human rights and freedoms

The use of the polygraph test has a number of implications related to the claims of limiting a number of fundamental rights and freedoms of the individual, such as:

Human dignity

Subjecting a person to a polygraph test treats them as an object rather than a subject. The results of these tests can be considered as evidence and if they show that he "did not pass the test", despite the fact that they are evaluated in the report and with the totality of other evaluations of the candidate, the latter can be seen as an unreliable person and without integrity, qualities related to reputation and respect for private and professional life.

The right to private and family life

This is because dignity accompanies every human being in exercising the

34 Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983, https://sgp.fas.org/othergov/polygraph/ota/index.html, accessed June 15, 2022

35 Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983, https://sgp.fas.org/othergov/polygraph/ota/index.html, accessed June 15, 2022

right to respect private and family life. The concept of private life is broad, so it is not subject to an exhaustive definition and can encompass multiple aspects of a person's physical and social identity. This right, as guaranteed by Article 8 of the ECHR, also protects the right to personal development and the right to create and develop relationships with other people and the outside world.Also, dignity affects the exercise of the right to work and profession.

The right not to incriminate oneself

The US Supreme Court has held that, in order for evidence to fall within the scope of the Fifth Amendment privilege (Right Against Self-Incrimination), it must be (1) incriminating, (2) testimonial, and (3) compelled.[36] Two of these conditions (incrimination and compulsion) are quite easy to identify. In fact, with respect to the current debate, all scholars agree that forcing a criminal defendant to submit to neuro lie detection qualifies as a form of compulsion, the purpose of which is to uncover incriminating evidence. Given the US Supreme Court's existing jurisprudence, there is no way to determine whether the results of neuro lie detection constitute testimonial evidence and would, therefore, be privileged under the Self-Incrimination Clause. [37]

In Schmerber, the Court recognized that the results of polygraph testing straddle the physical testimonial divide:

Some tests seemingly directed to obtain 'physical evidence,' for example, lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses which are essentially testimonial. To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment.[38]

In this passage, the Court indicates that even though physiological

36 See Fisher v. The United States, 425 U.S. 391, 408 (1976) ("The Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating.").

37 Neuro Lie Detection and Mental Privacy, Madison Kilbride, Jason Iuliano, Maryland Law Review, Volume 75, Issue 1, Article 5, 2015, https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3686&context=mlr, accessed 12 June 2022.

38 Schmerber, 384 U.S. at 764.

responses are physical in nature, the results of polygraph testing qualify as testimonials because they are designed to "elicit responses which are essentially testimonial."[39]

The right to due process

The respect for this right is questioned due to the use of the polygraph test as evidence in determining the person's integrity as a criterion for his employment in certain work positions, as well as the lack of effective legal mechanisms for contesting the result obtained through this test.

For example, when the necessary legal guarantees are not foreseen within the right to a regular legal process for citizens who are subject to the polygraph test, such as the right to be informed, heard, defended, complained about, etc. The employee who is evaluated does not have the right to dispute the data of the technological tools, the information or the report of the expert, or to dispute the expert himself.

The principle of equality before the law and non-discrimination

It is related to the claim that this test is mandatory for a certain category of job positions, and it is not so for another category of officials.

For example, in the case of the review by the Constitutional Court of the Republic of Albania of the request for the repeal of some provisions of law no. 95/2016 "On the organization and operation of institutions to fight corruption and organized crime", as well as Law no. 12/2018 "On the transitory and periodic evaluation of employees of the State Police, the Guard of the Republic and the Service for Internal Affairs and Complaints in the Ministry of the Interior".

The claim of the petitioners regarding the unequal treatment was related to the fact that the verification of the figure through the polygraph was necessary only for the candidates for the position of the head and the investigator in the National Bureau of Investigation and not also in the process of re-evaluation of the judges and prosecutors, who were to be selected in specialized institutions against corruption and organized crime,

39 Neuro Lie Detection and Mental Privacy, Madison Kilbride, Jason Iuliano, Maryland Law Review, Volume 75, Issue 1, Article 5, 2015, https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3686&context=mlr, accessed 12 June 2022.

in terms of verification of the figure.

Also, according to the petitioners, the use of these techniques constituted discrimination for the employees undergoing the test.

Conclusions

There are different approaches in different countries regarding the use of polygraph test as evidence in criminal proceedings, as well as in proceedings of an administrative nature, such as in employment relations in various positions of which are related to public security.

In relation to the latter, from a jurisprudential point of view, it is estimated that the polygraph test means an apparatus that continuously and simultaneously records both cardiovascular, respiratory, and electrodermal data. The test results can serve as data to determine the integrity of the person undergoing the procedure, based on the truthfulness of his answers. It is applied in labor relations only for certain public structures, which require in their ranks employees of high integrity.

Polygraph testing in the workplace is said to be highly contentious and controversial, as the admissibility and reliability of its results remain unclear. The credibility of the polygraph was challenged almost as soon as it was invented and the validity of a polygraph reading has been widely criticized.

Webliography

1. Scientific Validity of Polygraph Testing: A Research Review and Evaluation, A Technical Memorandum, Washington, D. C.: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983;

2. Chicago: Where Polygraph Becomes a Science, Stanley M. Slowik, Frank S. Horvath, EUROPEAN Polygraph, Volume 13, 2019, Number 1 (47);

3. An “Unfair and Cruel Weapon”: Consequences of Modern-Day Polygraph Use in Federal Pre-Employment Screening, Ariela Rutbeck-Goldman, IC Irvine Law Review, Vol. 7:715;

4. Deceptive or effective? Polygraph testing in the workplace, Hogan Lovells, April 2014;

5. Employee Polygraph Protection Act of 1988, Pub. L. 100-347, Sec.

1, 29 U.S.C. §§ 2001 et seq. Section 2001(3), enacted by the US Congress;

6. Polygraph for Sex Offender Management (Probation and Supervised Release Conditions), United States Courts;

7. The shaky science of lie detectors, Sandee LaMotte, CNN, September 7, 2018;

8. Can you catch a liar? How negative emotions affect brain responses when lying or telling the truth, Alice Mado Proverbio, Maria Elide Vanutelli, and Roberta Adorni, March 25, 2013;

9. Social and Cognitive Correlates of Children's Lying Behavior, Victoria Talwar, Kan Lee, October 30, 2012;

10. The brain adapts to dishonesty, Neil Garrett, Stephanie C Lazzaro, Dan Ariely & Tali Sharot, Nature Neuroscience, Volume 19, No.12, 2016;

11. Inconclusive: The truth about lie detector tests, Jennifer Vogel and Madeleine Baran, September 20, 2016;

12. Neuro Lie Detection and Mental Privacy, Madison Kilbride, Jason Iuliano, Maryland Law Review, Volume 75, Issue 1, Article 5, 2015;

13. How credible are lie detector tests? Gareth Evans, October 4, 2018, BBC News;

14. Brief history of the polygraph, Norman Kelly Polygraph Expert.

Court Decisions

1. US Supreme Court decision: Fisher v. The United States, 425 U.S. 391, 408 (1976);

2. Los Angeles Supreme Court decission: Los Angeles Police Protective League v. City of Los Angeles, 1995;

3. Montana Supreme Court decision: Oberg v. City of Billings, December 22, 1983;

4. Albanian Constitutional Court decision: no. 20, dated April 20, 2021;

5. Moldova Constitutional Court decision: no. 6 dated April 10, 2018.

THE ROLE OF TECHNOLOGY IN CRIMINAL PROCEEDINGS AND ITS IMPACT ON THE RIGHT TO PRIVACY. ANALYSIS OF JUDICIAL PRACTICE OF AMERICAN SUPREME COURT AND EUROPEAN COURT OF HUMAN RIGHTS.

MSC. KIARA MUKA

Ministry of Tourism and Environment in Tirana,

chiaramuka1@gmail.com

MSC. KLEA CAHANI

Center for Legal Civic Initiatives,

kleacahani.1@gmail.com

Abstract

As in any other field, technology and its latest innovations have become part of the justice system, including criminal justice. The use of technology in the latter plays an important role in terms of crime prevention, in facilitating investigative procedures, i.e. in the pre-trial phase, as well as in the judicial phase. However, it is noted that the involvement of technology in criminal proceedings is progressing at a faster pace than the drafting of accompanying legislation.

Creating such a situation, where legal provisions do not correspond to reality, makes it difficult to maintain a fair balance between the public interest in preventing or investigating crime, as well as the right to privacy of the suspect involved in these proceedings.

The purpose of this paper is to address the challenges that result from the use of technology in criminal proceedings towards respect for the right to privacy, bringing to attention the standards of the US Supreme Court and those of the European Court of Human Rights.

This paper will focus on research questions such as: How has technology influenced the achievement of the objectives of the criminal justice system? What limits exist in the power of technology to shrink the realm of guaranteed privacy? Does the use of these digital tools advance or hinder justice? What criteria will serve as the basis for the courts to weigh the protected public and private interest?

Due to the lack of Albanian case law in this area, we have chosen to address the court decisions of the Supreme Court of the United States of America, as well as the European Court of Human Rights, which have established a consolidated practice in this direction.

Key words: *technology, criminal procedure, privacy, case law, balance.*

1. Introduction

The fight against crime is one of the challenges facing today's European societies and beyond. Every day more and more such a fight depends largely on the use of advanced technological techniques in the prevention and investigation of crime. Such techniques have greatly facilitated the progress of crime prevention policies, as well as criminal processes of crime investigation and trial. However, the relevant legislation does not respond to innovations in scientific techniques of crime investigation. In this context, special attention is paid to the protection of the basic rights and freedoms of persons vulnerable to the use of these techniques.

The paper aims to provide a brief overview of some of the judicial decisions of the US Supreme Court and the European Court of Human Rights regarding the right to privacy, including the protection of personal data, the right to be forgotten, and the protection of correspondence and the inviolability of the dwelling.

Acquaintance with the developments of European Convention on Human Rights jurisprudence and the standards established by it from the interpretation of the rights guaranteed by the Convention takes on a special importance for our country, given that the limitations of the fundamental rights and freedoms of the ECHR arise in constitutional level[1].

1 Article 17, Constitution of the Republic of Albania provides*:*
"1. Restrictions of the rights and freedoms provided for in this Constitution can only be imposed

In addition, through this paper, it is intended to shed light on the impact that technology has had on the right to privacy over the years, as well as on the evolution of American judicial practice to adapt to these changes, but without infringing on the person's right to privacy. Regardless of the fact that these verdicts do not have a binding character for our state to implement them, they remain a very good judicial practice, as they set some very important standards for the guarantees of individuals and to control the legality of cyber actions that are carried out.

These judicial practices set a very good example, how the court, by maintaining the balances can fill legal gaps and prevent the use of these gaps in legislation to the disadvantage of individuals

2. Standards of the Supreme Court of the United States of America

2.1. *The right to privacy based on the US Constitution*

The Constitution of the United States of America, unlike the European Convention of Human Rights, does not explicitly include the right to privacy.[2] However, the Bill of Rights reflects the concern for protecting specific aspects of privacy, such as the privacy of beliefs (First Amendment), privacy of the home against demands that it be used to house soldiers (Third Amendment), privacy of the person and possessions as against unreasonable searches (Fourth Amendment) and the Fifth Amendment's privilege against self-incrimination, which provides protection for the privacy of personal information.[3]

Although there is no provision in the Constitution for the right to privacy, the Supreme Court, through its judicial practice over the years, has better portrayed the protection of this right and the standards that must be followed. In order to examine cases related to the right to privacy, the Supreme Court of the United States of America is based in the Fourth Amendment of the Constitution, which states that:

---

by law for a public interest or for the protection of the rights of others. The restriction must be proportionate to the situation that dictated it. 2. These restrictions cannot violate the essence of freedoms and rights and ***in no case can they exceed the restrictions provided for in the European Convention on Human Rights"***

2 Accessed from web page: https://www.law.cornell.edu/wex/right_to_privacy date 10.07.2022

3 Accessed from web page: http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html date 10.07.2022.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [4]

The Supreme Court, however, beginning as early as 1923 and continuing through its recent decisions, has broadly interpreted the Fourth Amendment to guarantee a broad right of privacy that has come to encompass different decisions.[5]

2.2. *The importance of "warrants" in order to protect the right to privacy. Inviolability of the home.*

The primary concerns of the generation that ratified the Fourth Amendment were "general warrants" and "writs of assistance." Today the Fourth Amendment is understood as placing restraints on the government any time it detains "seizes" or "searches" a person or property. The Fourth Amendment also provides *that "no warrants shall be issued, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."* The idea is that to avoid the evils of general warrants, each search or a judge should clear seizure in advance, and that to get a warrant the government must show "probable cause" a certain level of suspicion of criminal activity to justify the search or seizure.[6] The importance of obtaining a warrant, adds guarantees to the protection of the person's right to privacy in order not to allow abuse and to control the legality of the investigative actions that will carry out.

In the case ***Kyllo v. US***, the Court ruled that the authorities could not use without a warrant, a device that is not for public use, to understand what happens inside a private residence, even from the outside.[7] This case presents the question whether the use of a thermal-imaging device, aimed at a private home from a public street to detect relative amounts of heat within the home, constitutes a "search" within the meaning of the Fourth Amendment.

4 Accessed from web page: https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121 date 10.07.2022.

5 Accessed from the web page: http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html date 10.07.2022.

6 Accessed from web page: https://constitution.congress.gov/constitution/amendment-4/ date 10.07.2022.

7 Kyllo vs. US nr. 533-27 (2001), accessible on web page: https://supreme.justia.com/cases/federal/us/533/27/ date 05.07.2022.

Federal agents suspected that K. was growing marijuana in his home. They secretly placed in his office yard, a device that distinguished the heat. In this way, they aimed to determine if the heat emitted by the house was similar to that emitted by the high intensity lamps that are usually used to feed marijuana plants inside the house.[8] Despite the fact that the federal agents monitored only the outside of the office, the latest technological developments have made it possible for these devices to violate the privacy of individuals in an "indirect" way.[9]

In this context, the question that arises is how is it possible to protect the privacy of the person, in the conditions of the development of a world of high technology, where the police have electronic devices and computer skills that the creators of the Constitution could not have predicted.

Even though that the agents were protected by the fact that they only monitored outside the premises of the office, the Supreme Court stated, *"in the sanctity of the home, all the details are intimate".*[10] This establishes a very important principle, where the use of these electronic devices, not only should not violate the right to privacy as a whole, but also in particular should not violate the inviolability of the individual's home.

In this decision, the Supreme Court sets a very high standard, through which it not only aims to protect the individual's home, but also aims to protect the environment in which the person wants to be safe and not to be violated in his right to privacy. This means that the right to privacy is not related to the place, but to the person, and in whatever environment the person is, as long as he does not want to show his personal details, he must be protected. This principle is stated very clearly in the case ***Katz v. US.***

2.3. *The expansion of the concept of privacy. Secrecy of correspondence.*

What is concerning is the fact that the development of technology has

8 The Supreme Court in their verdict stated that the information received from these thermal devices in this case was the product of a "control". The authorities cannot use without a warrant a device that is not for public use, to understand what happens inside a private residence, even from the outside. If the authorities want to see what doesn't look clear from the outside, they should get a warrant. Kyllo v. US no. 533-27 (2001), accessible on web page: https://supreme.justia.com/cases/federal/us/533/27/ date 05.07.2022.

9 *"If the police will need a warrant to enter a residence, they will also need one to monitor from its exterior with high equipment"* Karo v. US no. 468-705 (1984) Accessed from the web page: https://supreme.justia.com/cases/federal/us/468/705/ date 07.07.2022.

10 Kyllo v. US no. 533-27 (2001), accessible on web page: https://supreme.justia.com/cases/federal/us/533/27/ date 05.07.2022.

exceeded the expectations and predictions of individuals, bringing many changes to society. Regardless of the provision in the Constitution or an Amendment, the concept of privacy has expanded today more that we could have imagined. For these reasons, there is a need to adapt the legislation with these changes, in order to protect the best interests of individuals.

The use of modern equipment facilitates even more the access of authorities or unauthorized persons to the correspondence of individuals. This makes them vulnerable against these measures, not only because they do not know that their correspondence is in interception, but also because even if they would know, they do not have the opportunity to defend themselves directly against these violations of their rights.

In the case ***Katz v. US***, the Supreme Court examined the nature of the right to a private life as well as the legal definition of control. Acting on suspicion that K. was transmitting gambling information over the phone to clients in other states, federal agents attached an eavesdropping device to the outside of a public phone booth, used by K. Based on the recordings he was convicted under an indictment for illegal transmission of wagering.[11]

These circumstances create ambiguity if the Fourth Amendment only protects the right to privacy of the person in his private premises, or will they be considered protected in public premises as well.[12] Discussing the scope of the Fourth Amendment, the court held that it protected individual privacy against certain types of governmental intrusions and not the right to privacy in general. The Fourth Amendment protected people and what they sought as private even in public places. It did not protect places *per se*. [13]

According to this, we understand that the Fourth Amendment protects people, not places.[14] What a conscious person shows in public, even if it is at home or in the office, is not protected by the Fourth Amendment. However, what the individual tries to keep as a private matter, must be constitutionally protected even in an area accessible to the public. The person, who uses a phone booth, closes the door and pays the fee to make the call, has the right

11 Katz v. US no. 389-347 (1967), accessible on web page: https://supreme.justia.com/cases/federal/us/389/347/ date 07.07.2022.

12 The Supreme Court in a 7-1 decision held that the use of an electronic device placed outside a public phone booth for overhearing conversations inside the booth, constituted "search and seizure", under the Fourth Amendment. The Court ruled that "search and seizure" was unlawful, and it was conducted without obtaining a prior warrant.

13 Katz v. US no. 389-347 (1967), accessible on web page: https://supreme.justia.com/cases/federal/us/389/347/ date 07.07.2022.

14 Ibid.

to assume that the words he will say on the phone will not be transmitted to other people. The fact that telephone booths are public should not infringe on the right to privacy of individuals because this right is related to people and not to the places where they are located.

If in 1967 there were cases on the use of telephone booths such as ***Katz v. US***, with the passage of time and with the development of technology, the number of cases where it was now about more complicated surveillance devices and methods, through which the right to privacy was violated, increased. Technological development led state authorities to develop more advanced tools to monitor individuals they suspected of criminal activity, for example to monitor their location and movements through their cell phones.

Regarding the protection of the correspondence of individuals, we find decisions that even confront each other, referring to the time in which they were taken. This shows that the development of technology has made it difficult to maintain an unwavering stance of the court, and the court in its decisions over the years has seen fit to adapt to technological advances, even though these decisions may be controversial with previous decisions.

If we refer to the case ***Smith v. Maryland***, the court, in the reasoning of the majority, did not find a violation of the applicant's right to privacy, even though in this case the individual's correspondence was exposed.

After the victim of a robbery began receiving phone calls from the person who claimed to be the robber, the police installed a pen register, without a warrant, at the central telephone system in order to determine the identity of the numbers that petitioner, a suspect, was dialing.[15]

The issues that raised these facts, laid out in the spectrum of if a pen register without a warrant violate the Fourth Amendment protection against unreasonable searches and seizures. The application of the Fourth Amendment embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy, whether the individual has shown that he seeks to preserve something as private.[16] The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as "reasonable", whether

15 After the police discovered that petitioner had called the victim, they charged him with robbery. Petitioner alleged that use of the pen register constituted an illegal search within the meaning of Fourth Amendment. Smith v. Maryland case no. 442-735 (1979), accessed from the web page: https://supreme.justia.com/cases/federal/us/442/735/ date 08.07.2022.

16 Accessed from the web page: https://www.lexisnexis.com/community/casebrief/p/casebrief-smith-v-maryland date 08.07.2022.

the individual's expectation, viewed objectively, is "justifiable" under the circumstances. Any claim of privacy must be "justifiable", "reasonable", or a "legitimate expectation of privacy" that has been invaded by government action.[17]

The court found that petitioner did not have a legitimate expectation of privacy regarding the numbers he dialed on his phone because those numbers were automatically turned over to a third party, the phone company.[18] Based on this argumentation, even if petitioner did harbor some subjective expectation that the phone numbers, he dialed would remain private, this expectation was not one that society was prepared to recognize as "reasonable".[19]

The ***Smith v. Maryland*** case raises the issue whether the phone records should be subject to the Fourth Amendment's protection. The court indeed arguments that the reasonable expectation of privacy does not apply to the numbers recorded by a pen register because those numbers are used in regular conduct of the phone company's business, which is a fact that individuals are aware of it. However, even though the individuals are aware of it, they actually do not have the opportunity to choose if they want to give their information to the companies or not. The individual's choice to voluntary turn over information is not valid because there is no practical alternative to it. These means that individuals should not be forced to accept the unfair conditions imposed by the government, where they are monitored through phone numbers or other data, without having the opportunity not to accept this. The fact that the citizen registers the phone number in a telephone company, according to the ***Smith v. Maryland*** case, means that your number will be automatically monitored if the government deems it necessary. This is the reason why the phone records should be subject to the Fourth Amendment protections, in a way that citizens do not feel violated and vulnerable.

Another case when the court discuss the issue of the secrecy of correspondence is the case ***Carpenter v. US***, in 2018. Differently from the ***Smith v. Maryland*** case, which was much earlier, in the ***Carpenter v. US*** case the court ruled that there was a violation of the Fourth Amendment of the Constitution.

The Supreme Court analysed if the warrantless "seizure and search" of historical cell-phone records revealing the location and movements of

17 Ibid.

18 Ibid.

19 Ibid.

a cell-phone user over the course of 127 days is permitted by the Fourth Amendment. The government obtained more than five months of historical cell phone location[20] records for 16 phone numbers from various wireless carriers.[21] With the location data provided by the carriers, the agents created maps showing that certain phones had been within a half mile to two miles of certain businesses around the times when robberies had occurred.[22] In this case the Supreme Court considered the Fourth Amendment standard for the use of mobile location data by law enforcements.[23]

However, the Supreme Court has not previously had an opportunity to address the application of the Fourth Amendment to many types of modern data, including cell phone location data. In the case ***Jones v. US*** in 2012, one of the Judges, remarked in her concurring opinion that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of in information voluntarily disclosed to third parties".[24] The court held that mobile location data is protected under the Fourth Amendment, declining to extend the "third-party doctrine" from ***Smith*** and ***Miller*** to this modern surveillance technique.[25]

The different decisions given in these two cases, which pertain to different time periods and very far from each other, show how the Supreme Court has changed its perspective and attitude towards the protection of the right to privacy of individuals, reflecting on technological changes. In addition, a further guarantee is given for the protection of the correspondence of individuals from the control of the authorities with various electronic devices.

20 The historical location data is the data that shows the prior connections to cell phone towers and/or antennas. Carpenter v. US case no. 16-402 (2018) Accessed from the web page: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf date 10.07.2022.

21 Carpenter v. US case no. 16-402 (2018) Accessed from the web page: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf date 10.07.2022.

22 The government later charged the defendants with six counts, including aiding and abetting robbery that affected interstate commerce. The Court held in a 5-4 decision that the government violates the Fourth Amendment to the United States Constitution by accessing historical records containing the physical locations of cellphones without a search warrant.

23 Ibid.

24 She describes this approach as *"ill suite to the digital age"* Jones vs US case nr. 357-493 (1958) Accessed from the web page: https://supreme.justia.com/cases/federal/us/357/493/ date 10.07.2022.

25 Ibid.

3. The right to respect for private and family life, under European Convention on Human Rights

The right to respect for private and family life is provided in Article 8 of the European Convention on Human Rights (hereinafter Convention or ECHR)[26]. Several rights derive from this article, including the right to respect for private life, family life, home and correspondence. The Convention provides the right to private and family life as a right with a non-absolute character. Therefore, according to paragraph 2 of Article 8 of the Convention, this right may be subject to interference. In this regard, the conventional provision has established several criteria, which are applied to any interference in the right to private life, guaranteeing the protection of this right from arbitrary interference. So, for every interference on the right to respect private and family life will be applied the following three tests:

- Is it in accordance with law?
- Does it pursue a legitimate aim?
- Is it necessary in democratic society?

The legitimate aims that an interference must pursue are provided in the second paragraph of Article 8 of the Convention, which are national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others. States enjoy a *'margin of appreciation'* when deciding on interference on the right to respect private and family life[27]. The width of the margin of appreciation varies from many factors related to the nature and importance of interference and their legitimate aim.

According to the focus of this scientific article, in order to address the respect for the right to privacy and the challenges arising in this regard from the use of advanced technologies in criminal proceedings, some of the decisions of the ECHR with this focus are addressed below.

---

26 Article 8 of the European Convention on Human Rights provides that: *"1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*, available at: https://www.echr.coe.int/documents/convention_eng.pdf, date 12.06.2022.

27 Guide on Article 8 of the European Convention on Human Rights, updated on 31 August 2018, available at: https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb, date 12.06.2022.

4. Standards of the European Court of Human Rights

4.1. *Retention, review and removed of personal data stored during a criminal procedure*

The protection of personal data is essential for respecting the right to private life. The sophistication of technology makes personal data even more sensitive.

In order to prevent crime in the country, the majority of the states have taken various measures, that also impact on the right to privacy. One of these measures is the creation of national electronic databases with personal data of people with a criminal past or suspected of committing a criminal offense. Different countries have had different regulations for the application of these measures. There have been many cases brought up for review before the European Court of Human Rights (hereinafter the Court/ECHR), whether the procedure selected by the states regarding the implementation of such measures for crime prevention were in accordance with the requirements of Article 8 of the Convention. In the following of the paper are addressed only some of the decisions, where the ECHR is expressed regarding this issue.

In the case of ***S. and Marper v. the United Kingdom***[28], the applicant S. was charged with attempted burglary when he was only 11 years old, while the applicant Marper was charged with threatening his partner. Both applicants were fingerprinted and DNA profiled in the criminal proceedings. After the conclusion of the criminal proceedings against them, S. and Marper requested that their personal data collected by the authorities in these proceedings be destroyed. They were unsuccessful because local law mandated the storage of these data without any time limit in a national database, which was regularly processed by automated means for criminal identification purposes.

In this case, the Court considered it appropriate to consider separately the issue of the interference with the applicants' right to respect for private life by the retention of cellular samples and DNA profiles on the one hand and fingerprints on the other. The court observed that: *"[...] profiles contain significant amounts of unique personal data [...] their processing through automated means allows authorities to go beyond neutral identification*[29]

28 S. and Marper v. United Kingdom, (No. 30562/04 & 30566/04), ECHR (2008), available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}, date 15.06.2022.

29 *The government admitted that the processing of DNA profiles could be used, and in some cases had been used, for family research to identify a possible genetic link between individuals. Also, the court observed that it is not disputed by the Government that the processing of DNA*

[...] The capacity of DNA profiles to provide a means of identifying genetic relationships between individuals is in itself sufficient to conclude that their retention interferes with the right to private life of the individuals concerned.[30]*"*

Regarding the keeping of fingerprints, the Court states that: *"the data of the applicants' fingerprints constitute their personal data, which contain some external identification features [...]* [31]*"* According to the Court, such data contain information target unique to the individual in question, allowing him to be accurately identified in a wide range of circumstances. Thus, according to the Court, they can influence private life and keeping this information without the consent of the individual in question cannot be considered neutral or irrelevant.

Regarding the implementation of such a measure by the United Kingdom, the Court saw with concern the fact that no distinction was made between suspected and convicted persons, it states that: *"Of particular concern in the current context is the risk of stigmatization, arising from the fact that persons in the position of the applicants, who have not been convicted of any criminal offense and have the right to the presumption of innocence, are treated in the same way. as convicted persons. [...]*[32]*"*

This practice chosen by the state was considered by the Court as not in accordance with the requirements of Article 8 of the Convention. For the Court, the general and indiscriminate nature of such a measure does not ensure the maintenance of a fair balance between public and private interests and constitutes a disproportionate interference in the applicants' right to private life, and it cannot be considered necessary in a democratic society[33].

In the case of ***B.B. v. France, Gardel v. France and M.B. v. France***, the Court concluded that a fair balance between the private interest (the right to the protection of personal data) and the public interest (the prevention of crime) has been achieved by the state. In this case, the Court took into consideration the fact that sexual crimes are a particularly punishable form of criminal activity, from which children and other vulnerable individuals

---

profiles allows the authorities to assess the possible ethnic origin of the donor and that such techniques are in fact used in police investigations. The possibility that DNA profiles create to draw conclusions about ethnic origin makes their retention even more susceptible to affecting the right to private life., para. 76 of the decision of court.

30 Ibid., para. 75.

31 Ibid., para. 81.

32 Ibid, para. 122.

33 Ibid, para. 125.

had the right to be effectively protected by the state. In addition, the court considered the fact that personal data was stored for convicted individuals for a period of 30 years and the local legislation had provided for an effective mechanism to enable the submission of a request for data deletion by the interested party, as well as wearing administrative authorities with the obligation to preserve data confidentiality. The legislator of the contracting state had even taken care to foresee in a detailed manner all the exceptional circumstances when access to these data could be allowed[34].

This position was further consolidated in 2013 by the European Court of Human Rights in the case of ***Peruzzo and Martens v. Germany***[35], where the court considered as clearly unfounded the request of applicants convicted of serious criminal offenses, personal data (DNA profile e) of which were kept in order to facilitate the investigation of possible crimes in the future[36].

In ***Catt v. United Kingdom***, the applicant Catt complained about the collection and storage of data in a police database on 'domestic extremists'. In assessing this case, the court took into consideration the fact that the applicant had never been convicted of any criminal offense, his advanced age and the existence of a risk to commit any crime on his part in the future, reaching the conclusion that keeping continuous data in this case was disproportionate. Also, the court criticized the lack of a time limit for keeping data, as well as the lack of effectiveness of the review mechanism[37].

In another case, in ***Gaughran v. United Kingdom***, the court held that the indefinite retention of biometric data (digital DNA profile, fingerprints) and photographs of persons sentenced to imprisonment for a criminal offense constituted a breach of the right to respect the private life of the person. The court criticized the fact that the data was kept for an indefinite time period as well as the lack of a real possibility of review. Also, the court emphasized

34 B.B. v. France (No. 5335/06), Gardel v. France, (No. 16428/05) and M.B. v. France (No. 22115/06) ECHR (2009).

35 Peruzzo and Martens v. Germany, (No. 7841/08 and 57900/12), ECHR (2013), available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-121998%22]} date 17.06.2022.

36 *DNA profiles could only be obtained from convicts who had committed serious or repeated offences; the time limit set for this purpose would not exceed ten years in relation to adults, taking into account in any case the purpose for which the data are stored as well as the nature and weight of the circumstances of the case; the applicants had the possibility of applying for the deletion of the stored data on the grounds that the legal requirements for their storage are not or are no longer met, and there was the possibility of a judicial objection (in the administrative courts) of the rejection of their request.*

37 Catt v. United Kingdom, (No. 43514/15), ECHR (2019).

that the seriousness of the offense[38] in question was not to the extent to justify an indefinite retention of sensitive data[39].

From the analysis of these decisions, we can highlight some of the standards that this court has established regarding the retention, review and remove of personal data stored during a criminal procedure. The court emphasizes in all cases the criterion of *"foreseeability* in the law, foresight of the way of applying advanced technological techniques in the prevention of crime, as well as their consequences with a sufficient precision. States should avoid legal provisions of a general nature in the implementation of such techniques, providing by law elements such as the following:

- The nature and seriousness of the criminal offences;
- The limit of the duration of data retention;
- The procedure to be followed for the collection, use and storage of the data received;
- The authority responsible for the administration of personal data;
- Right to data deletion or *"the right to be forgotten"*;
- Circumstances in which data deletion may be requested;
- An effective mechanism for administrative and/or judicial review.

The clear provision of such elements in the law constitutes an effective guarantee against the abuse of every individual's right to the protection of personal data, as well as a guarantee of the rule of law.

4.1.1. *Surveillance by GPS*

Data collected by a GPS device constitute personal data as far as they may indicate the whereabouts of an individual and his or her public movements. The ***Uzun v. Germany***[40] case was the first GPS surveillance case before the Court. From the study of this case, the objective evaluation criteria that the court examined have been identified, which are presented below:

- Such a measure served the interests of national and public security,

38 *Gaughran pleaded guilty and was fined for driving while intoxicated, and his driver's license was suspended.*

39 Gaughran v. United Kingdom, (No. 45245/15), ECHR (2020).

40 Uzun v. Germany (No. 35623/05), ECHR (2010), available at: https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22873181%22],%22itemid%22:[%22001-100293%22]} , date 31.06.2022.

crime prevention and the protection of victims' rights.

- It was a serious crime, GPS surveillance was ordered to investigate several allegations of attempted murder in order to prevent further terrorist attacks.
- Other less intrusive surveillance methods had proved insufficient.
- The GPS surveillance was carried out for a relatively short period of time (some three months) and not comprehensive (the person in question was only monitored when he was traveling in his accomplice's car)[41].

Therefore, the Court considers that the applicant's surveillance via GPS, as carried out in the circumstances of the present case, was proportionate to the legitimate aims pursued and thus *"necessary in a democratic society"* within the meaning of Article 8 § 2. There has accordingly been no violation of Article 8 of the Convention[42].

In the case of ***Ben Faiza v. France***, the French authorities, in order to destroy a large drug trafficking operation, had ordered the installation of a GPS in the vehicle of one of the Ben Faiza brothers[43]. The GPS device had enabled the authorities to track Mr. Ben Faiza in real time. The GPS was accompanied by the installation of another device to receive and record the conversations of the vehicle's occupants.

The Court noted in its assessment that the provision in France's Code of Criminal Procedure referred to a very general notion of *'acts of information considered useful for establishing the truth'*, and in its view did not provide the criterion of *"foreseeability"* required by Article 8 paragraph 2 of the Convention. For the Court, the lack of precision of the French law at the time in question could not be compensated by the case law of the domestic courts. According to her, to what extent and how the authorities had the right to use their discretionary power should have been clearly provided for in the procedural law[44]. In this case, the court found a violation of Article 8 of the Convention.

41 Ibid, para. 80.

42 Ibid, para 81.

43 *In 2009-2010, the Ben Faiza brothers were suspected of being involved in large-scale drug trafficking and were subjected to surveillance measures. In 2009, criminal police officers, with the authorization of the prosecutor, issued a court order to obtain recordings of incoming and outgoing calls. In 2010, the police were verbally authorized by the investigating judge to attach a tracking device to the vehicle of one of the brothers.*

44 Ben Faiza v. France (No. 31446/12), ECHR (2018), available at: BEN FAIZA c. FRANCE (coe.int) , date 31.06.2022.

4.2. *New technologies and the right to respect prisoners' correspondence*

The right to respect the confidentiality of correspondence and communications is enshrined in Article 8 of the Convention. The sophistication of technology has made this right even more vulnerable. In the following, we have selected two cases to address how the court handled the claim of the applicants for violating the right to respect correspondence.

In ***Helander v. Finland***, the prison authorities refused to transmit to the prisoner an e-mail sent by his lawyer to the prison e-mail address. For the prison authorities, such a refusal came because the legislation could not guarantee attorney-client confidentiality regarding such communications, in this case by e-mail. Therefore, the authorities immediately notify the lawyer of the failure to send the message and instruct him on the appropriate means of communication such as telephone, mail or visits to the prisoner[45].

Firstly, in this case the court stated that e-mail falls within the scope of 'correspondence', for the purposes of Article 8 of the Convention. The court declares that: *"[...] even though the electronic message in question was submitted to the prison's common electronic mailbox, it was nevertheless destined for the applicant and accompanied with a request that it be transmitted to him. There is therefore an issue about correspondence which falls within the scope of Article 8 and which the applicant may have the right to receive.[46]"*

Secondly, regarding the applicant's claim for violation of his right to respect correspondence from the authorities, the court examined some objective assessment criteria. In its assessment, the court considered the fact that there had been legitimate reasons for the refusal, the fact that the applicant's lawyer had been immediately informed of the non-delivery of the e-mail and had been instructed to use the appropriate means of communication, among which he had at his disposal effective and fast means of communication as well as e-mail. Thus, the Court assessed that: *"[...] having regard to the margin of appreciation left to the State, the Court considers that the refusal by the domestic authorities to transmit the e-mail message in question to the applicant cannot be regarded as unjustified for the purposes of Article 8 of the Convention.[47]"*

In conclusion, in evaluating the circumstances of the case, the court

45 Helander v. Finland, (No. 10410/10), ECHR (2013), available at: https://hudoc.echr.coe.intfre#{%22itemid%22:[%22001-127056%22]}, date 31.06.2022.

46 Ibid. para. 48.

47 Ibid. para. 56.

concluded that the state has reached a fair balance between the various interests involved.

In another case, ***Nuh Uzun and others v. Turkey***, the Court considered the uploading of detainees' private correspondence to a judicial IT server as an interference with the applicants' right to respect for their private life and correspondence[48].

In the Court's view, the documents that gave rise to the obligation to scan and upload all incoming and outgoing correspondence of detainees and prisoners, had thus been internal unpublished documents containing instructions from the Ministry of Justice to prisons. As a matter of principle, they did not have binding force. Thus, texts of this kind, which were not issued under any rule-making powers, could not be regarded as "law" of sufficient "quality" for the purposes of the Court's case-law, capable of affording adequate legal protection and the legal certainty necessary to prevent arbitrary interference by public authorities with the rights guaranteed by the Convention. Hence, the interference complained of could not be said to have been *"in accordance with the law"* within the meaning of Article 8 of the Convention. There had therefore been a violation of that provision[49].

5. Conclusions and Recommendations

At the end of this analysis, we can say that the Supreme Court and the ECHR, through their practice over the years, have opened the legal way to the examination of the right to privacy in relation to technological developments in such a way that the problems arising from these developments not to be left without a solution.

Therefore, the Convention, the Constitution must be seen as living documents and must be interpreted in the light of today's conditions and circumstances. Legislation must be able to adapt to changing situations in order to fulfil the guarantees of the rule of law.

The Supreme Court and the ECHR are clear indicators of how cases can be resolved even though there are no clear legal provisions. Also, the evolving jurisprudence of these courts, their detailed interpretation and reasoning help states to reflect in their domestic legislation the necessary

48 Nuh Uzun and others v. Turkey (No. 49341/18 and 13 other applications), ECHR (2022).

49 Ibid.

guarantees for the protection of the right to privacy.

Acquaintance with these standards is valuable in order to improve the current legislation and prevent similar issues from being subject to judicial review in the future.

The restrictions of human rights should be provided in the law with sufficient precision, avoiding measures of a general character and strengthening the necessary guarantees against the abuse of rights using the standards of these courts.

Bibliography references

Legislation:

- Constitution of the Republic of Albania.
- European Convention on Human Rights.

Decisions of US Supreme Court:

- Kyllo v. US no. 533-27 (2001).
- Katz v. US no. 389-347 (1967).
- Smith v. Maryland no. 442-735 (1979).
- Carpenter v. US nr. 16-402 (2018).
- Jones v. US nr. 357-493 (1958).
- Karo v. US nr. 468-705 (1984).

Decisions of the ECHR:

- S. and Marper v. United Kingdom, (No. 30562/04 & 30566/04), ECHR (2008).
- B.B. v. France (No. 5335/06), Gardel v. France, (No. 16428/05) and M.B. v. France (No. 22115/06), ECHR (2009).
- Uzun v. Germany, (No. 35623/05), ECHR (2010).
- Peruzzo and Martens v. Germany, (No. 7841/08 and 57900/12), ECHR (2013).
- Helander v. Finland, (No. 10410/10), ECHR (2013).

- Ben Faiza v. France (No. 31446/12), ECHR (2018).
- Catt v. United Kingdom, (No. 43514/15), ECHR (2019).
- Gaughran v. United Kingdom, (No. 45245/15), ECHR (2020).
- Nuh Uzun and others v. Turkey (No. 49341/18 and 13 other applications), ECHR (2022).

Web pages:

https://wwwnewlaw.wordpress.com/2020/12/09/provat-elektronike-ne-hetimin-penal/

https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

https://rm.coe.int/alb-2-intro-judicial-training-training-packs/1680a27040

https://qbz.gov.al/preview/b4819f4d-c246-49b3-87a9-2e6c8512c975

https://www.law.cornell.edu/wex/right_to_privacy

http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121

https://supreme.justia.com/cases/federal/us/533/27/

https://supreme.justia.com/cases/federal/us/468/705/

https://supreme.justia.com/cases/federal/us/389/347/

https://supreme.justia.com/cases/federal/us/442/735/

https://www.lexisnexis.com/community/casebrief/p/casebrief-smith-v-maryland

https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

https://supreme.justia.com/cases/federal/us/357/493/

https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb

HYRJA NDËRKUFITARE NË SISTEMET KOMPJUTERIKE DHE PARIMI I SOVRANITETIT SHTETËROR

MA. DITMIR HODA
Drejtoria e Përgjithshme e Doganave, Tiranë
Ditmirhoda@outlook.com

Abstract

The risk that computer networks and computer information may be used to commit criminal offenses, while related facts may be memorized, stored and transferred through these means is permanent and obvious[1]. The modern phenomena of digitalization, convergence and continuous globalization of computer networks[2] and computer data[3], have created a suitable ground for the commission of cybercrime, formatting its transnational character and transformed it into one of the typical forms of organized crime action.

The ability to quickly access computer data, which is found in other jurisdictions, is an important aspect of modern criminal investigations. However, the fact that prosecuting authorities have the capacity to conduct such searches does not make it permissible. This will usually be considered a violation of territorial sovereignty for those from a country conducting investigations in a foreign country without the authorization of that country.

Judicial practice has had cases in which courts order entities that are not

1 See the preamble of the Convention on "Crimes in the field of cybernetics."

2 "Computer system" means any device or group of interconnected or connected devices, one or more of ëhich, in continuation of a program, performs automatic data processing.

3 "Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, comprising a program suitable for the operation of a computer system to perform a function.

located in the territory of our country to make available computer data. Is it such thing legally justifiable?

Also the international character of cybercrime has led the jurisprudence to hold different positions regarding the criteria mentioned by the convention to determine which state party has jurisdiction, in cases where the action is carried out by a foreign citizen outside the territory and the consequence comes in the territory of another state.

Keywords: sovereignty, computer, jurisdiction, procedure, cybercrime.

1. Juridiksioni dhe kompetenca territoriale

Në terma të juridiksionit substancial, që është aftësia e shteteve të ushtrojnë juridiksion mbi veprat penale,[4] Konventa kërkon që palët, shtetet anëtare, të krijojnë një juridiksion mbi figurat e veprave penale të parashikuara në nenet 2-11 të konventës. E thënë ndryshe shtetet duhet të marrin nisma legjislative, nëpërmjet të cilave të bëhet e mundur zgjerimi i ushtrimit të juridiksionit penal për figurat e veprave penale të cituara në konventë. Ndërkohë që qëllimi është të ofrohet një aplikim sa më i gjerë të mundur, palët rezervojnë të dretën të mos aplikojnë apo të kufizojnë aplikimin, të ndonjë prej bazave juridiksionale të ndryshme nga territorialiteti.[5] Megjithatë Konventa nuk përjashton çdo juridiksion penal të ushtruar nga një shtet sipas ligjit të tij të brendshëm.[6] Kur më shumë se një palë pretendojnë juridiksion, ato duhet "të konsultohen për të përcaktuar juridiksionin më të përshtatshëm.[7] Megjithatë, Konventa mund të kritikohet për faktin që nuk parashikon ndonjë kriter për zgjidhjen e mosmarrëveshjeve të tilla.[8]

Në nenin 22 të Konvetën përcaktohen një sërë kriteresh, në bazë të cilave shtetët anëtare janë të detyruara të përcaktojnë juridiksionin mbi veprat penale të renditura në nenet 2-11 të Konventës[9].

4 *Shih "Comprehensive Study on Cybercrime*," 55.

5 Shih neni n 22/2 të Konventës . Në total, gjashtë vende kanë ushtruar këtë të drejtë në shkallë të ndryshme — Australia, Belgjika, Franca, Japonia, Mbretëria e Bashkuar dhe Shtetet e Bashkuara të Amerikës: shih Council of Europe, *List of Declarations Made with Respect to Treaty No 185* <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NTw185&CMW8&DF=&CL=ENG&VL>.

6 *Convention* art 22(4).

7 Ibid neni 22(5).

8 Henrik W K Kaspersen, 'Cybercrime and Internet Jurisdiction' (Discussion Paper (draft), Council of Europe, Project on Cybercrime, 5 March 2009) 20–2 [59]–[67].

9 Shih nenin 22 të Konventës "Për krimin në fushën e kibërnitikës", ratifikuar nga ana e vendit

Kriteret që ka parashikuar konventa janë kriteret tradicionale që parashikojnë ligjet e brendshme të shteteve anetare si:

- Parimi i territorialitetit. Paragrafi i parë i nenit të sipërcituar littera a bazohet në parimin e territorialitetit, duke parashikuar se secila palë duhet të ndëshkojë kryerjen e krimeve të parashikuara në këtë Konventë që janë kryer në territorin e saj. Për shembull, një palë do të pranojë juridiksion territorial në qoftë se personi që sulmon një sistem kompjuterik dhe sistemi viktimë janë të vendosur brenda territorit të tij, dhe në rastet kur sistemi kompjuterik i sulmuar është brenda territorit të tij, edhe në qoftë se sulmuesi nuk është[10].

Gjatë diskutimeve për hartimin e konventës u shqyrtua mundësia e përfshirjes së një dispozitë, e cila të obligojë shtetet palë që të shtrijnë juridiksionin mbi veprat penale të lidhura me satelitët e regjistruara në emër të palës. Hartuesit arritën në përfundimin se një dispozitë e tillë ishte e panevojshme, sepse komunikimet e paligjshme që përfshijnë satelitët, gjithmonë vijnë nga/dhe/ose merren në tokë. Si të tilla, një nga bazat për juridiksionin e një pale të përcaktuara në paragrafin 1 (a) - (c) do të jetë në dispozicion nëse transmetimi ka origjinë ose përfundon në një vendndodhje të përcaktuar aty. Gjithashtu për aq sa vepra përfshin komunikimin satelitor, i cili kryhet nga shtetasi i një pale jashtë juridiksionit territorial të çdo shteti, do të ketë një bazë juridiksioni sipas paragrafit 1(d). Hartuesit shtruan pyetjen: *Nëse regjistrimi ishte një bazë e përshtatshme për të pranuar juridiksionin penal pasi në shumë raste nuk do të ketë lidhje kuptimplotë mes veprës së kryer dhe Shtetit të regjistrit për shkak se një satelit shërben si një kanal i thjeshtë për transmetim?*

---

tonë me ligjin nr. 8888 datë 25.04.2002 "Për ratifikimin e "Konventës në fushën e kibertikës, të cilin theksohet se: "Juridiksioni 1. Secila Palë merr masa të tilla legjislative ose të tjera, që janë të nevojshme për të caktuar juridiksionin për çdo vepër penale të kryer në pajtim me nenet 2 –11 të kësaj Konvente, kur një vepër e tillë kryhet: a) në territorin e tij; ose b) në bordin e një anijeje që mban flamurin e asaj Pale; ose c) në bordin e një avioni të regjistruar sipas ligjit të kësaj Pale; ose d) nga njeri prej shtetasve të saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer ose nëse vepra është kryer jashtë juridiksionit territorial të çdo Shteti. 2. Secili Shtet mund të rezervojë të drejtën për të mos zbatuar ose për të zbatuar vetëm në raste të caktuara ose kushte të caktuara rregullat juridiksionale të parashikuara në paragrafët (1)b – (1) d të këtij neni ose të ndonjë pjese të tyre. 3. Secila Palë merr masa të tilla që janë të nevojshme për të caktuar juridiksionin mbi të gjitha veprat penale të përmendura në nenin 24, paragrafi (1) i kësaj Konvente, në rastet kur kryrësi i prezumuar i veprës penale është prezent në territorin e saj dhe ajo nuk e ekstradon atë tek një Palë tjetër, kryesisht mbi bazën e shtetësisë së tij/saj pas kërkesës së bërë për ekstradim. 4. Kjo Konventë nuk përjashton asnjë juridiksion penal të ushtruar në pajtim me ligjin vendas. 5. Nëse më shumë se një Palë pretenton juridiksionin mbi një vepër që prezumohet e kryer në pajtim me këtë Konventë, Palët e interesuara, kur është e përshtatshme, bëjnë një konsultë për të përcaktuar juridiksionin më të përshtatshëm për të bërë ndjekjen penale.

10 Shih raportin shpjegues.

Paragrafi 1, *litterae b* dhe *c* janë të bazuara në një variant të parimit të territorialitetit. Këto *littera e* kërkojnë që secila palë të pranojë juridiksionin penal mbi veprat e kryera mbi anijet që mbajnë flamurin e saj ose avionë të regjistruar sipas ligjeve të saj. Ky detyrim është tashmë i zbatuar si një cështje e përgjithshme, në ligjet e shumë shteteve, pasi këto anije dhe avionë janë konsideruar shpesh si një zgjatje e territorit të shtetit[11]. Ky lloj juridiksioni është më i dobishëm dhe i përdorshëm kur anija ose avioni nuk janë vendosur në territorin e shtetit në kohën e kryerjes së krimit, si rezultat i së cilës Paragrafi 1, *littera a* nuk do të jetë në dispozicion si një bazë për pranimin e juridiksionit. Në qoftë se krimi është kryer në një anije ose avion që është jashtë territorit të palës së flamurit, nuk mund të ketë shtet tjetër që do të mund të ushtrojë juridiksionin bazuar në këtë kërkesë. Më tej, në qoftë se një krim është kryer në bordin e një anijeje ose avioni i cili është thjesht duke kaluar nëpër ujërat ose hapësirën ajrore të një shteti tjetër, ky i fundit mund të përballet me pengesa të rëndësishme praktike për ushtrimin e juridiksionit të tij, dhe prandaj është e dobishme që edhe shteti i regjistrimit të ketë juridiksion.

- Paragrafi 1, *littera d* bazohet në parimin e shtetësisë. Teoria e shtetësisë është më shpesh e zbatueshme nga Shtetet që aplikojnë traditën e civil law. Ajo parashikon që shtetasit e një Shteti janë të detyruar të zbatojnë të drejtën e brendshme, edhe kur ata janë jashtë territorit të saj[12].
- Sipas *littera d*, në qoftë se një shtetas kryen një vepër penale jashtë vendit, Pala është e detyruar të ketë aftësinë për të ndjekur penalisht atë, nëse sjellja është gjithashtu një vepër penale sipas ligjit të shtetit në të cilin është kryer ose kur veprimi ka ndodhur jashtë juridiksionit territorial të çdo shteti.
- Paragrafi 2 lejon Palët të bëjnë një rezervë për bazat e juridiksionit të përcaktuara në paragrafin 1, *litteraeb, c* dhe *d*. Megjithatë, nuk është e lejuar asnjë rezervë në lidhje me juridiksionin territorial sipas *littera a*, ose në lidhje me detyrimin për ushtrimin e juridiksionit në rastet që bien nën parimin e "*aut dedere aut judicare*" (ekstrado ose ndiq penalisht) sipas paragrafit 3, kur një palë ka refuzuar të ekstradojë të dyshuarin në bazë të kombësisë së tij dhe autori është i pranishëm në territorin e saj. Jurisdiksioni i përcaktuar në bazë të paragrafit 3 është i nevojshëm me qëllim që palët që refuzojnë ekstradimin e një shtetasi, të kenë aftësinë ligjore për të ndërmarrë hetimet dhe procedurat në

11 Po aty.

12 Shih nenin 22/1/d të Konventës.

vend, në qoftë se kërkohet nga Pala që ka kërkuar ekstradimin në përputhje me kërkesat e "Ekstradimit", neni 24, paragrafi 6 i kësaj Konvente.

Bazat e juridiksionit të përcaktuara në paragrafin 1 nuk janë ekskluzive. Paragrafi 4 i këtij neni lejon shtetet palët, që të krijojnë, në përputhje me legjislacionin e tyre të brendshëm, lloje të tjera të juridiksionit penal.

Në rastin e krimeve të kryera me anë të përdorimit të sistemeve kompjuterike, do të ketë raste në të cilat më shumë se një palë do të ketë juridiksion mbi disa ose të gjithë pjesëmarrësit në krim. Për shembull, shumë sulme virusesh, mashtrime dhe shkelje të drejtave të autorit kryer nëpërmjet përdorimit të viktimave e targetuara në Internet, të vendosura në shumë shtete. Për të shmangur dyfishimin e përpjekjeve, shqetësimet e panevojshme për dëshmitarët, apo konkurrencën mes zyrtarëve të zbatimit të ligjit në Shtetet e lidhura, ose për të lehtësuar efikasitetin apo ndershmërinë e procesit, Palët e prekura duhet të konsultohen në mënyrë që të përcaktojnë vendin e duhur për ndjekje.

Në disa raste, do të jetë më efektive për shtetet e interesuara për të zgjedhur një vend të vetëm për ndjekjen; në disa të tjera, mund të jetë më e mira për një shtet që të ndjekë penalisht disa pjesëmarrës, ndërsa një ose disa Shtete të tjera të njekin të tjerët. Së fundi, detyrimi për t'u konsultuar nuk është absolut, por duhet të ndodhë "kur është e përshtatshme." Kështu, për shembull, në qoftë se një nga Palët e di se konsultimi nuk është i nevojshëm (psh, ka konfirmim se Pala tjetër nuk ka në plan të ndërmarrë veprime), ose në qoftë se një Palë është e mendimit se konsultimi mund të dëmtojë hetime apo procedimin e saj, ajo mund të shtyjë ose të refuzojë konsultimin.

Në kuadër të detyrave të marrë përsipër nga RSH me ratifikimin e konventës legjislacioni shqipëtar ndërmori nismat e duhura ligjore. Kështu me ligjin nr. 10023, datë 27.11.2008, nenin 7 të Kodit Penal është shtuar germa J: "j) vepra penale në fushën e teknologjisë së informacionit.".

Pyetja që lind është: Duke u bazuar në kriteret e sipërpërmendura cili shtet palë ka juridiksion, në rastet kur një shtetas që ndodhet në territorin e një shteti pale nëpërmjet përdorimit të sistemit kompjuterik me anë të gënjeshtrës vjedh pasurinë e shtetasve, të cilët ndodhen në territorin e një shteti tjeter? Pra në rastet kur veprimi kryhet nga një shtetas i huaj jashtë territorit dhe pasoja vjen në territorin e një shteti tjeter?

Një shtet do të ketë juridiksion territorial, edhe në qoftë se krimi është kryer jashtë territorit të tij, për sa kohë që një element konstituiv i figurës së

vepres penale është kryer në atë Shtet. Në doktrinën juridke ky është quajtur juridiksioni territorial subjektiv. Juridiksioni territorial subjektiv, është variabël nga provueshmeria se elementi i krimit dhe krimi në vetvete janë krejtësisht të pandashëm. E thënë ndryshe nëse do të mungonte elementi përbërës, krimi nuk do të kishte ndodhur.

Këtë qëndrim ka mbajtur edhe Gjykata Ndërkombëtare e Drejtësisë(GJND)[13], në çeshtjen "Lotus" (France vs Turkey) (Judgment) të vitit 1927, Nr 10, në të cilën thekson se: *"Turqia dhe Franca të dyja kishin juridiksion në lidhje me incidentin: dmth kanë juridiksion konkurrues....*

Vepra ka prodhuar efektet e saj në anije turke dhe si pasojë në një vend të asimiluar me territorin turk, në të cilin zbatimi i ligjit penal turk nuk mund të kundërshtohet, madje edhe në lidhje me vepra penale të kryera atje nga të huajt. Pra, nëse një akt i kryer në det të hapur prodhon efektet e tij në një anije që mban flamur të një shteti të huaj ose në territor të huaj, të njëjtat parime duhet të zbatohen si në qoftë se territoret e dy shteteve të ndryshme janë të prekura, dhe konkluzioni duhet pra të jetë se nuk ka rregulla të ligjit ndërkombëtar që ndalojnë shtetin e anijes në të cilën efektet e veprës penale kanë ardhur, për ta konsideruar rastin si vepër penale të kryer në territorin e tij dhe për të ushtruar ndjekjen penale, në përputhje me rrethanat……..

Vepra penale për të cilën Lieutenant Demons është ndjekur penalisht ishte një akt - i neglizhencës apo pakujdesisë - që ka origjinën e vet në bordin e Lotus, ndërsa efektet e aktit janë ndier në bordin e Boz-Kourt. Këto dy elemente janë, ligjërisht, në tërësi të pandashme, aq shumë sa ndarja e tyre e bën veprën penale joekzistente... Është e natyrshme që secili shtet duhet të jetë në gjendje për të ushtruar juridiksion dhe për ta bërë këtë në lidhje me këtë incident si një e tërë. Prandaj është një rast i juridiksionit konkurrues. ".

Të njëjtin qëndrim, por duke përdorur argumenta të tjerë, ka mbajtur edhe Gjykata e Lartë e Shtetëve të Bashkuara të Amerikës. Kështu në rastin[14] United States v Ivanov, ajo theksoi se: "*rastet e mëparshme përbënin precedent për aplikimin e juridiksionit ekstraterritorial, për sa kohë që "efekte e dëshiruara dhe të dëmshme" kanë ndodhur brenda juridiksionit".*

Gjykata duke iu referuar precedentit United States v. Muench, theksoi se: "*Qëllimi për të shkaktuar efekte brenda Shteteve të Bashkuara, e bën të arsyeshme zbatimin për personat jashtë territorit të Shteteve të Bashkuara*

13 Shih Vendimin e Gjykatës Ndërkombëtare të Drejtësisë (GJND), çeshtja "Lotus" (France vs Turkey) (Judgment) të vitit 1927, Nr 10, 18–19.

14 Shih United States v Ivanov, 175 F Supp 2d 367 (D Conn, 2001).

të një statuti që nuk është shprehimisht ekstraterritorial në fushëveprim". Gjykata, gjithashtu, duke iu referuar precedentit United States v. Steinberg, argumentoi se:" *….Ka qenë prej kohësh e zakonshme dhe e pranuar përgjegjësia penale e një personi, i cili mund të akuzohet në vendin ku rezultojnë pasojat, edhe pse ai është jashtë juridiksionit në momentin kur ai fillon trenin e ngjarjeve, frut i të cilave është pasoja e ardhur*. "

Gjykata argumentoi se efektet e dëmshme të sulmeve të Ivanov në të vërtetë kanë ndodhur në Shtetet e Bashkuara, duke deklaruar se: "*..Fakti që kompjuterët janë aksesuar me anë të një procesi kompleks të iniciuar dhe kontrolluar nga një vend i largët nuk e ndryshon faktin se aksesimi i kompjuterëve, pra, pjesë e efektit të dëmshëm të ndaluar me statut, ka ndodhur në vendin ku kompjuterët janë të vendosura fizikisht, dmth në vendndodhjen e OIB, pra në Vernon, Connecticut. Në një argument të dytë, gjykata deklaroi se pavarësisht logjikës së mëparshme, "në secilën prej statuteve për të cilat i pandehuri është akuzuar për një vepër materiale, ka prova të qarta se statuti kishte për qëllim për tu aplikuar ekstraterritorialisht*."

2. Parimet bazë të bashkëpunimit ndërkombëtar

Nëse veprimet e kundërligjshme në fushën e teknologjisë dhe informacionit kryhen në nivel kombëtar, trajtesa e tyre materiale substanciale dhe procedurale penale, "fuqia hetimore" mund të bëhet pa iu drejtuar marrëveshjeve ndërkombëtare. Kur këto vepra dhe procedura duhet të aplikohen jashtë juridiksionit, marrëveshjet ndërkombëtare marrin një rëndësi vendimtare. Aftësia për të kryer hetime që prekin apo ndikojnë në territorin e shteteve të tjera, i ashtuquajturi 'juridiksioni hetimor'[15], është trajtuar në mënyrë të hollësishme nga konveta[16].

Konventa nuk parashikon shprehimisht parimin e reciprocitetit[17], por kërkon që palët të bashkëpunojnë me njëra-tjetrën "sa më shumë që të jetë e mundur" në hetimin e krimit kibernetik dhe mbledhjen e provave elektronike[18]. Kjo përfshin shkëmbimin e informacionit pa kërkesë kur do të ndihmojë një tjetër palë në hetimin e tij ose që besohet se mund të ndihmojë

15 Shih United Nations Office on Drugs and Crime,'Comprehensive Study on Cybercrime' (Report, February 2013)1 ('Comprehensive Study on Cybercrime'),55.

16 Shih kapitullin 3 të saj.

17 Në kontrast, United Nations Convention against Transnational Organized Crime, hapën për nënshkrim në 12 Dhjetor 2000, 2225 UNTS 209 (hyri në fuqi në 29 Shtator 2003) neni 18(1) ('UNTOC') parashikon se palët "duhet reciprokisht të shtrijnë me njeri tjetrin asistencë të ngjashme" kur ka baza të arsyeshme për të dyshuar se vepra ka natyrë transnacionale.

18 Convention neni 23.

palën pritëse në hetimin e ndonjë vepre që mund të cojë në një kërkesë për ndihmë të ndërsjellë në bazë *Konventës*[19].

Natyrisht, jo të gjitha hetimet mund të kryhen në baza informale ose vullnetare, prandaj janë bërë parashikime në *Konventë* për ndihmë të ndërsjellë. Këto parashikime pasqyrojnë fuqitë (kompetencat) procedurale të diskutuara më sipër, duke përfshirë ruajten e përshpejtuar të të dhënave kompjuterike të ruajtura dhe zbulimin e përshpejtuar të trafikut të të dhënave[20]. Në rastin e mbledhjes në kohë reale të të dhënave të trafikut dhe përgjimit të të dhënave të përmbajtjes, palët do të japin një ndihmë të tillë siç lejohet sipas ligjeve të tyre të brendshme dhe traktateve të zbatueshme (subjekt i rezervave të parashikimeve të Konventës)[21]. Në përputhje me parimin e përgjithshëm në nenin 23, palët janë gjithashtu të ofrojnë ndihmë reciproke "sa më shumë të jetë e mundshme" në lidhje me "veprat penale që lidhen me sistemet kompjuterike dhe të dhënat, ose për mbledhjen e provave në formë elektronike për një vepër penale"[22]. Fillimisht, dispozita bën të qartë se bashkëpunimi ndërkombëtar duhet të sigurohet mes Palëve "në masën më të gjerë të mundshme. Ky parim kërkon që palët të sigurojnë bashkëpunim të gjerë me njëra-tjetrën, dhe të minimizojnë pengesat për rrjedhjen e shpejtë të informacionit dhe provave ndërkombëtarisht.

Si me bashkëpunimin vullnetar, kjo pikë e fundit njeh se bashkëpunimi efektiv ndërkombëtar është i rëndësishëm jo vetëm për 'krimin kibernetik' në kuptimin e ngushtë, por për të gjitha veprat penale që përfshijnë prova dixhitale.[23]

Së dyti, qëllimi i përgjithshëm i detyrimit për të bashkëpunuar është përcaktuar në nenin 23: Bashkëpunimi duhet të shtrihet në të gjitha veprat penale që lidhen me sistemet kompjuterike dhe të dhënat kompjuterike (p.sh.Veprat që mbulohen nga neni 14, paragrafi 2, *litterae a-b*), si dhe për mbledhjen e provave në formë elektronike për një vepër penale. Kjo do të thotë se pavarësisht nëse krimi është kryer nga përdorimi i një sistemi kompjuterik, ose kur një krim i zakonshëm nuk është kryer nga përdorimi i një sistemi kompjuterik (psh, një vrasje) por përfshin prova elektronike, kushtet e Kapitullit III janë të aplikueshme. Megjithatë, duhet theksuar se nenet 24 (Ekstradimi), 33 (Ndihma e ndërsjellë në lidhje membledhjen e të dhënave të trafikut në kohë reale) dhe 34 (Ndihma e ndërsellë në lidhje me

19 Ibid neni 26.

20 Ibid nenet 29–30.

21 Ibid nenet 33–4.

22 Ibid neni 25(1).

23 Convention Explanatory Report, [243], [253].

mbledhjen e të dhënave të përmbajtjes) lejojnë palët të ofrojnë një fushë të ndryshme të aplikimit të këtyre masave.

Megjithatë palët mund të kufizojnë nivelin e tyre të bashkëpunimit më ngushtë në rastet e ekstradimit, ndihmës së ndërsjellë në lidhje me mbledhjen në kohë reale të të dhënave të trafikut dhe ndihmës reciproke në lidhje me përgjimin e përmbajtjes së të dhënave.[24] Më gjerë, ky parim i përgjithshëm i bashkëpunimit duhet të bëhet "përmes aplikimit të instrumentave relevant ndërkombëtar për bashkëpunim ndërkombëtar në cështjet penale, marrëveshjeve të arritura në bazë të legjislacionit uniform ose reciprok, dhe ligjeve të brendshëm".[25] Kjo përforcon parimin e përgjithshëm se bashkëpunimi në bazë të kap.III nuk i zëvendëson këto instrumente dhe marrëveshje të tjera.[26]

Së fundi, bashkëpunimi duhet të kryhet "në përputhje me dispozitat e këtij Kapitulli" dhe "përmes zbatimit të marrëveshjeve përkatëse ndërkombëtare për bashkëpunimin ndërkombëtar në cështjet penale, marrëveshjeve të arritura në bazë të legjislacionit uniform ose reciprok dhe ligjet e vendit." Klauzola e fundit krijon parimin e përgjithshëm se dispozitat e kreut III nuk zëvendësojnë dispozitat e marrëveshjeve ndërkombëtare për ndihmën e ndërsjellë ligjore dhe ekstradimin, marrëveshjeve reciproke midis palëve, ose dispozitat relevante të ligjit të brendshëm që kanë të bëjnë me bashkëpunimin ndërkombëtar. Ky parim themelor është përforcuar në mënyrë të qartë në nenet 24 (Ekstradimi), 25 (Parimet e Përgjithshme në lidhje me ndihmën e ndërsjellë), 26 (Informacionet spontane), 27 (Procedurat në lidhje me ndihmën e ndërsjellë për kërkesat në mungesë të marrëveshjeve ndërkombëtare të aplikueshme), 28 (Konfidencialiteti dhe kufizimi i përdorimit), 31 (Ndihma e ndërsjellë sa i përket aksesit në të dhënat kompjuterike të memorizuara), 33 (Ndihma e ndërsjellë në lidhje me mbledhjen e të dhënave të trafikut në kohë reale) dhe 34 (Ndihma e ndërsjellë në lidhje me mbledhjen e të dhënave të përmbajtjes).

Për të lehtësuar bashkëpunimin, formal dhe joformal, *Konventa* gjithashtu parashikon krijimin e një rrjeti 24/7, ku secila palë cakton një pikë kontakti, që të jenë në dispozicion në çdo kohë, për të ofruar ndihmë të menjëhershme për qëllime të hetimeve të krimit kibernetik ose procedurat për mbledhjen e të dhënave elektronike.[27] Kjo dispozitë është e bazuar në përvojën e rrjetit të

24 Shih Part (II).

25 Convention neni 23.

26 Convention Explanatory Report, [244].

27 Convention neni 35.

pikave të kontaktit të G8, të cilat aktualisht përbëhet nga 50 anëtarë.[28]

Nëse zbatohet, një nga ndryshimet më të rëndësishme që mund të rezultojë nga Konventa do të jetë përpunimi i përshpejtuar i kërkesave urgjente të ndihmës reciproke. Mekanizmat aktualë të ndihmës reciproke janë tejet të ngadalshme, dhe mund të duhen muaj pasi kalojnë nëpërmjet kanaleve burokratike duke përdorur mjetet tradicionale.[29] Konventa bën parashikime për palën, në "rrethana urgjente", që të bëjnë kërkesa dhe komunikime për të ndihmë të ndërsjellë duke përdorur "mjete të përshpejtuara të komunikimit, përfshirë faks ose e-mail".[30] Këto mjete duhet të shfrytëzohen vetëm në masën që ato të sigurojë nivelet e duhura të sigurisë dhe autenticitetit.[31] Pala e kërkuar duhet të pranojë dhe ti përgjigjet kërkesës duke përdorur mjete të përshpejtuara të komunikimit, me konfirmim formal të nevojshëm vetëm në qoftë se e kërkon pala e kërkuar.[32]

3. Ndihma reciproke dhe objekti i saj

Edhe pse palët duhet të bashkëpunojnë "sa më shumë të jetë e mundshme"[33], nuk ka asnjë detyrim për të dhënë informacion në mënyrë spontane, dhe çdo ofrimi informacionit është subjekt i së drejtës së brendshme të palës ofruese. Më tej, një informacion i tillë mund të ofrohet duke iu nënshtruar kushteve të detyrueshme, për shembull, konfidencialitetit.[34] Kjo është vecanërisht e rëndësishme kur dhënia e informacionit mund të zbulojë informacione operacionale të tilla si aftësia teknike apo teknikat, ose subjektin e hetimeve.[35] Megjithatë, është inkorporimi i ndihmës së ndërsjellë dhe dispozitave të ekstradimit që mund të ngrenë shqetësime deri në masën se cili ligjit i brendshëm do të aplikohet për të vepruar me urdhër të agjencive të zbatimit të ligjit të huaj.

---

28 Council of Europe, Action against Economic Crime: About 24/7 Points of Contact <http://ëëë. coe. int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp>. Shih gjithashtu Interpol I-24/7 Secure Global Police Netëork: Interpol, Data Exchange <http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7>.

29 Convention Explanatory Report, [256].

30 Convention neni 25(3). Ka patjetër shembuj ilustrues,të cilët do të zhvillohen me zhvillimin e teknologjisë. ibid [256].Për shembull, Voice over Internet Protocol (VoIP) mund të përdoreet si një formë komunikimi.

31 Convention Explanatory Report, , [256].

32 Ibid.

33 *Convention* nenet 23, 25.

34 Ibid neni 26(2).

35 *Convention Explanatory Report*, [261].

Në përgjithësi, Konventa nuk imponon detyrime për ndihmë reciproke te palët. Përvec se kur është parashikuar ndryshe, ndihma e ndërsjellë i nënshtrohet ligjeve të brendshme të palës së kërkuar ose traktateve në fuqi të ndihmës reciproke, duke përfshirë edhe arsyet për të cilat pala e kërkuar mund të refuzojë bashkëpunimin.[36]

Kjo i lejon palët të ofrojnë masa mbrojtëse të përshtatshme në lidhje me personat e vendosur Brenda juridiksionit të tyre.[37] Megjithatë, kjo është subjekt i kualifikimit "përvec kur parashikohet ndryshe specifikisht".[38] Për shembull, në lidhje me veprat penale sipas neneve 2-11 të Konventës, ndihma e ndërsjellë nuk duhet të refuzohet vetëm me arsyen se kërkesa ka të bëjë me një vepër penale që pala e kërkuar e konsideron të jetë një "vepër fiskale"[39]. Kjo "reflekton shqetësimin në rritje se veprat me natyrë fiskale, të tilla si pastrim parash, janë komponentet kryesore të krimit të organizuar ndërkombëtar dhe për këtë arsye nuk duhet të jetë imun ndaj hetimit, ekstradimit dhe ndjekjes".[40]

Duke aplikuar parimin e subsidiaritetit, Konventa gjithashtu mund të plotësojë marrëveshjet e tjera multilaterale ose bilaterale mes shteteve, ose mund të përdoret aty ku nuk ka marrëveshje të tilla në fuqi.[41] Për shembull, ajo është përdorur së bashku me Konventa e Kombeve të Bashkuara kundër Krimit të Organizuar ('UNTOC'), si dhe me marrëveshje ekstradimi bilaterale.[42] Megjithatë, këto marrëveshje nuk duhet të konflikohen me parimet e Konventës.[43] Nëse masa të tilla nuk janë në fuqi, ose masat ekzistuese nuk përmbajnë dispozita të përshtatshme, palët është e nevojshme të miratojnë

36 *Convention* nenet 25(4); ibid [254]. Një qasje e tillë është adoptuar edhe në *UNTOC*: shih *Manual on Mutual Legal Assistance and Extradition*, 22.

37 *Convention Explanatory Report*, [257]. Në disa juridiksione, ndihma e ndërsjellë dhe ekstradimi mund të lejohen nga ligji kombëtar pa referim në tractate: shih *Manual on Mutual Legal Assistance and Extradition*, 22 [53].

38 *Convention* neni 25(4).

39 Ibid. Megjithëse jo i përkufizuar në Konventë,janë përkufizuar në instrumenta të tjerë si 'shkelje në lidhje me taksat, detyrimet, doganat dhe këmbimin valuator Ibid. Although not defined in the *Convention*, these have been defined in other instruments as 'offences in connection ëith taxes, duties, customs and exchange': *European Convention on Extradition* neni 5.

40 *Manual on Mutual Legal Assistance and Extradition*, 53.

41 *Transborder Access and Jurisdiction Discussion Paper*, 18 [84].

42 Konferencë e Palëvë të Konventës Së Kombeve të Bashkuara kundër Krimit të Organizuar Transnacional, *Catalogue of Cases Involving Extradition, Mutual Legal Assistance and Other Forms of InternationalLegal Cooperation Requested on the Basis of the United Nations Convention Against TransnationalOrganized Crime*, 5th sess, Agenda Item 6, UN Doc CTOC/COP/2010/CRP.5 (22 September 2010) 5 [20], 8 [37] ('*Catalogue of Cases*').

43 *Convention* neni 23, 39.

masa të tilla legjislative të nevojshme për të përmbushur detyrimet e tyre.[44]

Ku kriminaliteti i dyfishtë është një kusht për ndihmën e ndërsjellë në bazë të ligjit ose detyrimeve te palës së kërkuar, dhe kjo është e lejuar në bazë të Konventës, ky kusht duhet të përmbushet "pavarësisht nëse ligjet e vendosin veprën në të njëjtën kategori shkeljes ose emërtojnë veprën me të njëjtën terminologji si pala kërkuese".[45] Kjo nuk do të imponojë kriminalitetin e dyfishtë në rastet kur sjellja nuk është vepër penale në të dy vendet. Përkundrazi, si me ekstradimin,[46] siguron se kërkesat për ndihmë të ndërsjellë nuk do të refuzohen për shkak të dallimeve në klasifikim por për kundërshtime substanciale.[47]Për shembull, ndërsa disa juridiksione e kanë adresuar keqpërdorimin e informacionit të identitetit në dispozitat specifike të "vjedhjes së identitetit", shumica vazhdojnë të mbështeten në një kombinim të mashtrimit dhe veprave të lidhura.[48] Për aq kohë sa sjellja është e kriminalizuar në të dy vendet, atëherë kriminaliteti i dyfishtë do të merret i përmbushur pavarësisht sesi është klasifikuar.

Në rast se nuk ka traktate të ndihmës apo marrëveshje në mes palëve, neni 27 i Konventës përcakton bazën mbi të cilën do të trajtohen kërkesat e ndihmës së ndërsjellë.[49]

Palët mund të refuzojnë ndihmën nëse kërkesa ka lidhje me një shkelje që pala e kërkuar e konsideron si vepër politike,[50] ose e konsideron kërkesën "si të rrezikshme për sovranitetin e saj, sigurinë, rendin publik apo interesa të tjerë thelbësore."[51] Gjithashtu, mund të shtyjë veprimet mbi një kërkëse nësë një veprim i tillë mund të dëmtojë hetimet penale apo procedurat e kryera nga autoritetet e tij."[52]

---

44 Ibid neni 25(2). Në disa raste, është e mjaftueshme që pala të trajtojë parashikimet e Konventës si vetë ekzekutuese, ose rregullimet ekzistuese mund të jenë mjaftueshëm fleksibël për të pranuar parashikimet e Konventës. Shih *Convention Explanatory Report*, [255].

45 *Convention* neni 25(5).

46 Shih Part II(B)(3).

47 *Convention Explanatory Report*, [259].

48 Neil Robinson, 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report' (Report No TR-982-EC, RAND Europe, June 2011) 80.

49 Këto parashikime mund të aplikohen në tërësi ose pjesërisht kur marrëveshje të tilla janë në fuqi ose ekzistojnë, por vetëm me marrëveshje të palëve në fjalë. Shih *Convention* neni 27(1). Shih *Convention*neni 28, që bën parashikime mbi konfidencialitetin dhe kufizimet që përdoren në të tilla rrethana.

50 Ibid neni 27(4)(a).

51 Ibid neni 27(4)(b).

52 Ibid neni 27(5).

Parashikime specifike janë bërë në lidhje me forma të caktuara të kërkesave për ndihmë të ndërsjellë.[53] Një palë mund të bëjë një kërkesë për ruajtje të përshpejtuar të të dhënave të regjistruara kur pala kërkuese do të paraqesë kërkesë për ndihmë të ndërsjellë për akses në ato të dhëna.[54] Ruajtja duhet të bëhet për të paktën 60 ditë në mënyrë që të lejojë palën kërkuese të bëjë kërkesën për akses në të dhëna.[55] Pasi një kërkesë e tillë është pranuar, të dhënat duhet të vazhdojnë të ruhen në pritje të një vendimi mbi atë kërkesë.[56] Kur kërkesa ka të bëjë me ruajtjen e të dhënave të trafikut dhe "pala e kërkuar zbulon se një ofrues shërbimi në një tjetër shtet ishte i përfshirë në transmetimin e komunikimit, pala e kërkuar duhet të zbulojë në mënyrë të përshpejtuar palës kërkuese një sasi të mjaftueshme të të dhënave të trafikut për të identifikuar ofruesin e shërbimit dhe rrugën përmes së cilës komunikimi ishte transmetuar".[57] Një kërkesë e tillë mund të refuzohet vetëm mbi baza se kërkesa lidhet me një shkelje politike, ose përndryshe do të "dëmtonte sovranitetin e saj, sigurinë, rendin publik apo interesa të tjera thelbësore."[58]

Edhe pse kriminaliteti i dyfishtë nuk është një kusht për të siguruar ruajtjen e tillë,[59] një palë që kërkon kriminalitetin e dyfishtë si kusht për t'iu përgjigjur kërkesave për ndihmë të ndërsjellë mund të rezervojë të drejtën të refuzojë mbi këtë bazë, nëse ka arsye të besojë se gjendja e kriminalitetit të dyfishtë nuk do të përmbushet në kohën e zbulimit.[60]

Ky kufizim nuk zbatohet për veprat penale të parashikuara në nenet 2-11, pasi palët duhet të kenë parashikuar vepra të tilla sipas ligjeve të tyre të brendshme.

Në të gjitha rastet, një kërkesë ruajtje mund të refuzohet mbi bazën se kërkesa ka të bëjë me një vepër penale politike, ose përndryshe do të "cenojë sovranitetin e saj, sigurinë, rendin public apo interesa të tjerë thelbësore".[61] Pasi këto dispozita shprehimisht përcaktojnë vetëm bazat mbi të cilat kërkesat do të refuzohen, ata veprojnë me përjashtim të ndonjë traktati

53 Ibid kap III s 2 title 1.
54 Ibid neni 29(1).
55 Ibid neni 29(7).
56 Ibid.
57 Ibid neni 30(1).
58 Ibid neni 30(2).
59 Ibid neni 29(3).
60 Ibid neni 29(4).
61 Ibid neni 29(5).

ekzistues të ndihmës reciproke, ose marrëveshjeje.[62] Megjithatë, pasi natyra e kërkesave bëhet më e ngarkuar, respekt më i madh i jepet marrëveshjeve ekzistuese dhe / ose ligjeve kombëtare. Për shembull, neni 30, i cila ka të bëjë me ndihmën e ndërsjellë në lidhje me aksesin në të dhënat kompjuterike të ruajtura, nuk bën asnjë parashikim në lidhje me arsyet e refuzimit. Arsye të tilla do të gjenden në traktatet ekzistuese ose në bazë të nenit 27. Neni 33, i cili ka të bëjë me ndihmën e ndërsjellë në mbledhjen e të dhënave të trafikut në kohë reale, është përcaktuar specifikisht që të rregullohet nga kushtet dhe procedurat e parashikuara nga ligjet kombëtare. Forma më e shpeshtë e kërkesës, përgjimi i të dhënave të përmbajtjes, është e rregulluar plotësisht nga "traktatet e zbatueshme dhe ligjet brendshme".[63]

Konventa parashikon që objekt i **ndihmës së ndërsjellë të jetë marrja e masave të përkohshme.** Kështu një Palë mund t'i kërkojë një Pale tjetër të urdhërojë ose të sigurojë në ndonjë mënyrë tjetër ruajtjen e përshpejtuar të të dhënave të regjistruara nëpërmjet një sistemi kompjuterik, i cili ndodhet brenda territorit të Palës tjetër dhe në lidhje me të cilën Pala dërguese ka ndërmend të bëjë një kërkesë për ndihmë të ndërsjellë për të kërkuar hyrje të ngjashme, ngrirje, sigurim të ngjashëm ose hapje të të dhënave[64]. Një mekanizëm i tillë në nivel ndërkombëtar është ekuivalent me atë të parashikuar në nenin 16 të Konventës për përdorimin në nivel kombëtar.

Konkluzione:

- Dimensioni transnacional që ka fituar sot krimi kompjuterik karakterizon çdo veprimtari hetimore që, edhe kur zhvillohet ende në nivel lokal, priret të marrë tipare përtej territoriale, bashkëpunimi ndërkombëtar përfaqëson një parakusht për çdo veprimtari të përbashkët lufte.
- Një vepër penale ka një natyrë ndërkombëtare në qoftë se kryhet në më shumë se një shtet, ose kryhet në një shtet, por pjesa thelbësore e përgatitjes, planit, drejtimit ose kontrollit është ndërtuar në një shtet tjetër, ose kryhet ne një shtet, por në të është përfshirë një grup kriminal i organizuar, i cili angazhohet ne aktivitete kriminale në më shumë se një shtet, ose kryhet në një shtet, por pasojat thelbësore i ka në një shtet tjetër. Karakteri transnacional i krimit komjuterik derivon juridiksionin e një

62 Ibid neni 25(4).

63 Ibid neni 34.

64 Shih nenin 29/1 të Konvetës "Për krimin në fushën e kibërnitikës", ratifikuar me ligjin nr 8888 datë 25.04.2002

shteti për të ushtruar ndjekjen penale për këtë krim.

- Ndërhyrja ndërkufitare nënkupton qasjen në mënyrë të njëanshme të të dhënave kompjuterike të ruajtura në një shtet palë tjetër pa kërkuar ndihmë të ndërsjellë juridike. Këta terma i referohen të dhënave të ruajtura kompjuterike të vendosura në një Palë tjetër. Kërkimet ndërkufitare të pambuluara nga Konventa nuk janë "as të autorizuara, as të përjashtuara".
- Komiteti duhet të marrë në konsideratë hartimin e një projekt-udhëzimi në lidhje me adoptimin e qasjes ndaj ndërhyrjes ndërkufitare. Madje kërkohet që të hartohet një protokoll shtesë i konventës kundër krimin kibernetik mbi kufijtë e ndërhyrjes ndërkufitare, i cili do të ishte i nevojshëm.

Biblografia:

- S.Schjolberg,"The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva", 2008,
- Making the weorld safer from drugs, crime and terrorism - The European Union (EU) and the United Nations Office on Drugs and Crime (UNODC), 2015,
- David Felsen, Akis Kalaitzidis " A historical overvieë of transnational crime",
- Bossard A., Transnational Crime and Criminal Laë, University of Chicago, Office of international Criminal Justice, 1990,
- Mueller, G.O, Transnational Crime Definitions and Concepts, 2001,
- Serrano,M., Transnational organized crime and International Security: Business as usually, 2002,
- Sheptycki, J., Against transnational organized crime, University of Toronto Press, 2003,
- Itali-Shqipëri: Instrumente ligjorë dhe teknika të luftës kundër krimit të organizuar transnacional përballje përvojash nën kujdesin e Corrado Lembo, Koordinator shkencor i Kursit të trajnimit për gjyqtarë, prokurorë dhe oficerë të policisë gjyqësore (Tiranë, 5-16 mars 2007; Romë, 15-19 tetor 2007; Tiranë, 12-16 nëntor 2007),
- Agnés Cadet-Taïrou and others, "Substances psychoactives, usagers et marchés: les tendances récentes (2015-2016)", Tendances, vol. 8, No. 115 (December 2016).
- Europol, IOACTA 2016: Internet Organized Crime Threat Assessment,

The Hague, 2016.

- "Police warning after drug traffickers' cyber-attack", 16 October 2013, BBC News. Available at http://www.bbc.com/ news/world-europe-24539417. Aksesuar më 14.04.2018.
- Cadet-Taïrou and others, "Substances psychoactives, usagers et marchés: les tendances récentes".
- Transnational Organized Crime: A Growing Threat to National and International Security, retrieved from http://m.whitehouse.gov/ administration/ eop/nsc/transnational-crime/threat.
- Internet World Stats, Albania, aksesuar më
- 13/11/2014, http://www.internetworldstats.com/euro/al.htm.
- Fabian Zhilla Besfort Lamallari "Vlerësimi Riskut të Krimit të Organizuar në Shqipëri" Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015.
- Trafficking in Human Beings: Internet recruitment. 2007 Council of Europe.
- Royal Canadian Mounted Police, Protocol on Foreign Criminal Investigators in Canada (15 February 2007) <http://www.rcmp-grc.gc.ca/interpol/fcip-pcece-eng.htm>.
- Teresa Scassa, Robert J Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction' (2011) 42 Georgetoën Journal of International Laë 1017, 1029.
- Jonathan Clough "A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation". Monash University laë revieë Vol 40 no 3,
- Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).
- Putin Defies Convention on Cybercrime', CNews (online), 27 March 2008 . See also Cybercrime Convention Committee (T-CY),
- 'Report on the 2nd Multilateral Consultation of the Parties d Strasbourg, 13 and 14 June 2007' (Information Document No CM/Inf(2007)38, Council of Europe, 20 July 2007) [6]
- generally United States v Gorshkov (WD Ëash, No CR00-550C, 23 May 2001); United States v Ivanov, 175 F Supp 2d 367 (D Conn, 2001).
- Convention Explanatory Report, above n 25, [293]. Convention art

39(3) provides that '[n]othing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

- Susan W Brenner and Joseph J Schwerha IV, 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime' (2002) 20 John Marshall Journal of Computer and Information Law 347.
- Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).

Legjislacion:

- Konventa "Për krimin në fushën e kibërnitikës", ratifikuar me ligjin nr. 8888 datë 25.04.2002
- Konventa kundër krimit te organizuar ndërkombëtar, e ratifikuar me ligjin nr. 8920, datë 11.7.2002.

Jurisprudencë:

- Vendimi i Gjykatës Ndërkombëtare të Drejtësisë (GJND), çeshtja "Lotus" (France vs Turkey) (Judgment) të vitit 1927, Nr 10, 18–19.
- Vendimi Shtetet e Bashkuara kundër Ivanov, 175 F Supp 2d 367 (D Conn, 2001)
- Vendimi Shtetet e Bashkuara të Amerikës, v. Stephen MUENCH, Defendant-Appellant. 97-2304. No. Decided: September 10, 1998

Adresa:

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf akses 13 Shtator 2018.

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf akses 13 Shtator 2018.

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 akses 13 Shtator 2018.

ROLI I TEKNOLOGJISË NË PARANDALIMIN DHE LUFTIMIN E KRIMIT TË ORGANIZUAR, KRIMEVE FINANCIARE DHE KORRUPSIONIT.

INTELLECTUAL PROPERTY RIGHTS AND LEGAL PROTECTION, HIGH TECHNOLOGY CRIMES.

MSC. ANA RUSHITI

Studente pranë Shkollës kombëtare të Avokatisë ,Tiranë

anarushiti25@gmail.com

Informacion biografik për autoren

Ana Rushiti ka lindur më 09/01/1998 në Gjirokastër . Arsimin fillor dhe të mesëm e kam mbarruar në qytetin e Gjirokastrës . Arsimin e lartë e kam mbarruar pranë Kolegjit Universitar të Biznesit ,Tiranë me rezultate shumë të mira . Gjithashtu kam mbarruar dhe studimet master shkencor në "E drejtë civile dhe tregtare" pranë këtij Kolegji duke marrë dhe çertifikatën e ekselencës.

Gjithashtu kam marrë pjesë në shume trajnime që kanë të bëjnë me fushën e bizneseve,motivimit ,vetëdisplinimit ,në fushën politike por duke mos lënë mënjanë trajnimet profesionale të kryera brenda ,por edhe jashtë vendit në fushën penale në Argjentinë . Gjithashtu jam angazhuar në ndihmë të familjeve në nevojë . Kam marrë pjesë në konferenca studentore kombëtare dhe ndërkombëtare .

Aktualisht ndjek shkollën e avokatisë .Gjithashtu kam publikuar dhe punim shkencor në revistë ndërkombëtare IJRDO me temë "Arbitrage ,an efficent alternative for resolving trade disputes in Albania comparative overëieë with Austria ,Armenia ,Argentina and Bulgaria" ISSN 2456-2971 vol7

Abstract

Albania is a country where very little has been said about intellectual and industrial property. The chosen topic is a necessary topic to be addressed as intellectual property is in great need of experts in this important field. Many certain individuals make works like in music, in various arts, poetry, various scientific articles, the production of a trademark in the market, but they do not know their rights and obligations arising from intellectual property. In this paper it is important treatment of the albanian legal framework versus the european legal framework related to intellectual property. The study of European Union directives and international court decisions is very important as it helps us make the necessary changes in the law by applying the principle of proportionality.

It is also important in case of copyright infringement to have legal protection. Legal protection can be done with a lawyer or self-defense. Legal protection is very important as it is a principle recognized by the European Convention on Human Rights (KEDNJ).

We live in the digital age where every service is available online, but high technology has brought many problems ranging from the physical and psychological formation of the child to the copyright infringement. This is a global issue and many websites have tried to protect the rights of copyright or inventor. Dealing with cases in a practical way would make the work more interesting, but also more practical.

I have participated in conferences such as the NATO Model Conference, National and International Student Conferences and I have also conducted training in the field of legal protection of authors & inventors. In the trainings I participated in I received an important message was “Motivation is the important weapon of success”.

Keywords: Rights, directives, development, technology, protection.

Hyrje

Pronësia intelektuale dhe industriale përbën një nga temat më të rëndësishme e cila ka marrë një zhvillim kohët e fundit. Zhvillimi i teknologjisë moderne ka bërë që të realizohen edhe vepra penale në fushën teknologjike .

Pronësia intelekturale dhe industriale kontribuon në mënyrë të drejtëpërdrejtë në sjelljen e një produkti me vlerë në tregun shqiptar dhe jo vetëm . Gjithmonë ka lindur nevoja dhe domosdoshmëria për njohjen dhe rëndësinë e pronësisë intelektuale dhe industriale pasi shumë kompani ,autorë të ndryshëm nuk e dinë mënyrën e mbrojtjes së të drejtave të tyre përballë personave të tjerë .Rëndësia e pronësisë intelektuale dhe industriale qëndron në koston e investimit për produktin . Teknologjia e informacionit po zhvillohet në përmasa të mëdha dhe lind nevoja për produkte të reja efektive ,cilësore ,por edhe moderne .

Pronësia intelektuale ndikon edhe në botën e veprave letrare ,shkencore dhe materialeve muzikore . Shqipëria ka pasur problem të theksuar plagjiaturën e temave të doktoraturave gjë,e cila me ligjin e arsimit të lartë të Republikës së Shqipërisë u ndalua plagjiatura dhe ka filluar një riorganizim i ri për studimet doktorale .Përveç kësaj studentët kur realizojnë temat e diplomave bachelor apo master ka pasur raste që nuk e kanë referuar burimin se ku e kanë marrë . Gjithashtu edhe në gazetari shumë artikuj nuk e kanë referencën apo burimin e informacionit dhe vërtetimi i informacionit është i rëndësishëm pasi informon publikun . Gjithashtu ka kompani të cilat kanë të njëjtën logo apo treguesi gjeografik nuk është i saktë . Tek pronësia intelektuale dhe industriale konkurrenca është mjaft e rëndësishme ku çmimet ,shërbimi dhe cilësia bëjnë diferencën .

Krimet e teknologjisë së lartë kanë ndikuar negativisht në kryerjen e veprave penale duke favorizuar shumë individë të ndërhyjnë në ndryshimin ,kopjimin dhe marrjen pa autorizimin e autorit apo shpikësit veprën letrare ,shkencore dhe produktin e përftuar .Lufta kundër krimeve të teknologjisë së lartë nuk është arritur të mposhtet nga vendet e botës ku Rusia dhe SHBA janë më të prekurat ,por nuk përjashtojmë edhe vende të tjera . Shqipëria është treguar mjaft e dobët në mbrojtjen e të drejtave të autorit duke mos ndjekur mekanizmat mbrojtës të veprave letrare ,muzikore apo shkencore. Shqipëria ka ligje të posaçme lidhur me pronësinë intelektuale dhe industriale.Ligji nr 35/2016 “Për të drejtën e autorit dhe të drejtat e tjera dhe ligji nr 9947 datë 27/4/2008 “Për pronësinë industriale” Qëllimi i këtyre ligjeve ka qenë mbrojtja ligjore e autorëve të veprave letrare ,muzikore shkencore por edhe

të shpikësve .Duhet pasur parasysh tek e drejta e autorit mbrohen të drejtat jo pasurore duke respektuar cilësinë e autorëve në lidhje me interesat e tij ekonomike.

I Të drejtat dhe detyrimet që rrjedhin nga pronësia intelektuale dhe industriale mbrojtja ligjore

1.1 Të drejtat që rrjedhin nga pronësia intelektuale dhe industriale

Të drejtat që rrjedhin nga pronësia intelektuale dhe industriale :

1) **E drejta e mbrojtjes - 1**Mbrojtja e veprave artistike,shkencore ka të bëjë që asnjë autor & person tjetër nuk ka të drejtë ta modifikojë ,ndryshojë veprën e autorit .Nëse vepra e autorit nuk arrin të mbrohet atëherë do të ketë përfitime për palën tjetër dhe humbje për palën e autorit .Gjithashtu edhe vepra e autorit mund të përdoret për qëllime të tjera për të ndikuar në imazhin pozitiv të autorit duke i sjellë si pasojë një imazh negativ në publik. Ata nuk munden të përdorin vepra të caktuara pa miratimin e autorit apo dhe të agjensive të menaxhimit kolektiv të cilët kanë për detyrë për të menaxhuar të drejtën e autorëve.

2Mbrojtja e pronësisë industriale(markat ,patentat,shpikjet) bëhet nëpërmjet patentave ku patenta jepet duke marrë parasysh disa kushte : të përbëjë risi,të përmbajë hap shpikës,të jetë e zbatueshme në industri. Përjashtim shpikje nuk konsiderohet zbulimet ,teoritë shkencore metodat matematike,krijimet estetike ,skemat dhe rregullat për kryerjen e veprimeve mendore për zhvillimin e lojrave dhe biznesit si dhe programet kompjuterike.

2) **E drejta morale -** Nënkupton të drejtën e autorit dhe të rishikimit por nuk ka të bëjë me botimin e veprës. E drejta morale ka të bëjë dhe mbrojtjen nga shtrembërrimet që mund t'i bëhen veprës dhe si e tillë mbrojtja e dinjitetit të autorit të veprës.

3) **E drejta pronësore -**E drejta pronësore përfshin të drejtën e përkthimit ,riprodhimit ,të përformacës publike ,të transmetimit ,të drejtën e përshtatjes ,rinovimit .3Liria e shprehjes është nga liritë themelore të japë dhe të marrë

1 https://ascap.edu.al/wp-content/uploads/2018/02/Pronesia-intelektuale-dhe-indusstriale-P%C3%ABrmbajtja-e-modulit.pdf datë 13.6.2022

2 Neni 5 dhe 6 i Ligjit nr 9947 datë 7/7/2008 "Për Pronësinë Industriale

3 Neni 1 i Konventës Europiane për të drejtat e Njeriut

informacion dhe për të dhënë mendim pa kufizim të autoriteteve publike dhe pa marrë parasysh kufijtë .Kjo ka lidhje kryesisht me transmetimet audiovizive,televizive ose konematografikedhe duhet të pajisen me licensë.

4) **E drejta e revokimit së autorësisë -** Autori e ka të drejtën e revokimit të veprës së tij në rast se ka arsye serioze morale me kusht që të kompensohet dëmi real të shkaktuar nga revokimi i së drejtës .Bartësi i së drejtës duhet ta njoftojë autorin e veprës lidhur me masën e dëmit të pësuar nga revokimi i dëmit.

5) **E drejta ekonomike -** Autorët e veprave & shpikjeve të ndryshme kanë të drejtë të përfitojnë nga produktet e tyre dhe madje produkti i tyre është konkurrues në tregun ndërkombëtar. Çdo vepër & shpikje ka koston e vet në nxjerrjen e saj në treg dhe si e tillë autori ka të drejtë të mbrojë koston ekonomike dhe të marrë mbrapsht atë që ka investuar .Një nga liritë e rëndësishme është liria ekonomike dhe si e tillë teknologjia në një farë mënyre ka arritur që vepra kryesisht të artit&botime shkencore libra dhe shpikjet e ndryshme kanë arritur të përdorin dhe shitjen online ..Konkurrenca është mjaft e rëndësishme,por kompanitë autorët e veprave shpikjeve nuk mund të shkelin rregullat e konkurrencës.

6) **E drejta për patentë -** është një e drejtë e rëndësishme që i takon shpikësit për të pasur një patentë dhe në rast se është zëvendësuesi i tij ligjor rregullohet me marrëveshje ndërmjet tyre .Kur kemi 2 ose më shumë aplikime për të njëjtën shpikje përparësi do ketë ai aplikant që ka apikuar për këtë shpikje në një datë më të hershme.

7) **E drejta për të ndaluar përdorimin tërthorrazi të shpikjes -** Pronari i shpikjes ka të drejtë të ndalojë çdo palë të tretë të drejtën e shftytëzimit të shpikjes për të cilën është dhënë patenta .Kjo do të thotë që vetëm pronari ka të drejtën eksluzive për të kaluar të drejtën e shfrytëzimit tek personat e tretë nëpërmjet kontratës së licensimit &marrëveshjes së licensimit.

8) **E drejta për shpërblimin e dëmit -** Pronari i shpikjes apo autori i veprës ka të drejtë të kërkojë shpërblimin në gjykatë ndaj veprës së tyre në rast se dëmi është real ,efektiv duke përfshirë edhe fitimin e munguar edhe duke ardhur si rezultat i shkeljes së konkurrencës dhe duke marrë në

konsideratë edhe dëmin moral . Në çdo rast gjykata civile është kompetente për vendosjen e masës së shpërblimit të dëmit.

1.2 Detyrimet që rrjedhin nga pronësia intelektruale dhe industriale:

a) Të zbatojë me përpikmëri kontratën &marrëveshjen e licensimit që ka me personin tjetër që merr të drejtën e shfrytëzimit të veprës në rastin e së drejtës së autorit për dorëzimin e dorëshkrimit brenda afatit të arsyeshëm dhe marrëveshjen e licensimit që ka pronari i patentës me persona të tretë .

b) Shpikësi është i detyruar të zbatojë procedurën për dhënien e një patente.

c) Të shpërblejë autorin & shpikësin e veprës letrare ,artistike,shkencore dhe të shpërblehet dëmi që mund të jenë shkaktuar nga konkurrenca e pandershme ose nga dëmi moral në marka ,dizenjo industriale tregues gjeografikë,patentë

d) Të paguajë taksat e padisë në gjykatë dhe taksat institucionale për depozitimin e kërkesave për aplikim.

e) Pronari i patentës ka detyrimin të njoftojë të licensuarin për gjykimin në fjalë.

1.3 Mbrojtja ligjore e pronësisë intelektuale dhe industriale .

1. Mbrojtja e pronësisë intelektuale bëhët kur mbajtësi i së drejtës së autorit ka bërë një kërkesë në gjykatë për masën e sigurimit të padisë ku dyshohet se janë cënuar të drejtat e tij ose kur ka raste se dyshohet se të drejtat e paditësit cënohen dhe objekti i kërkesë padisë është i pamundur ose i vështir ,një masë e përkohshme do të evitonte dëmin e cila do ishte e pariparueshme . Sigurimi i padisë në vetëvete është një masë parandaluese e cila do ndalonte pasojat negative që do të vinin nga ky veprim .Gjykata në këtë rast ka të drejtë të kërkojë pushimin dhe tërheqjen respektivisht të veprimeve apo të akteve e palës kundërshtare që shkelin të drejtën e autorësisë . 4 Gjithashtu edhe në rastin e shpërblimit të dëmit kundërvajtësi është i detyruar të shpërblejë autorin e veprës me vlerën përkatëse të përcaktuar prej tyre ose nga gjykata e cila mban parasysh shkallën e dëmit të shkelësit dhe shuma për të cilën është rënë dakord .

4 Neni 172Ligjit nr 35/2016 “ Për të drejtat e autorit dhe të drejta të tjera të lidhura me to”

2 Mbrojtja ligjore e pronësisë industriale (patentat,dizenjot industriale,markat dhe treguesit gjeografikë mbrohet nga Drejtoria e Përgjithshme e Pronësisë Industriale .5Mbrojtja ligjore fillimisht bëhët në rrugë institucionale që i drejtohen institucionit përkatës kërkesë për aplikim për markë tregtare ,dizenjo industriale dhe kjo kërkesë mund të pranohet ,mund të refuzohet ose mund të pezullohet.6Kundërshtimi për mbrojtjen e një patente mund të bëhet brenda 9 muajve nga data e publikimit dhe depozitimi për kundërshtim bëhet në bordin e apelimit të Drejtorisë së Përgjithshme të Pronësisë Industriale pasi të jetë bërë pagesa e tarifës së caktuar.Bordi i Apelimit mund ta shfuqizojë patentën ose të refuzojë marrjen e kërkesës.

3 Procedura gjyqësore fillon me ngritjen e padisë ndaj kudo që ka shkelur të drejtat apo që rrezikon të shkelë ndaj patentës, por jo vetëm . Në gjykatë duhet të provohën që shkelja ka ndodhur ose duhet të ndodhi ,duhet të provohet fakti që shkelja është bërë e përsëritur.kur shkelja ka ndodhur në cënim . Në këto raste gjykata mund të vendosë në varësi të rrethanave të rastit 1) sigurimin e padisë dhe marrjen e masave të përkohshme 2) shpërblimin e dëmit7 3) vendos pushim cënimi për çdo veprim që përbën shkelje të së drejtës së patentës.8Përsa i përket parashkrimit së të drejtës për të kërkuar dëmshpërblim bëhët brenda 3 viteve nga data kur personi ka marrë dijeni ose duhet të kishte marrë dijeni për dëmin e pësuar dhe për personin që e ka shkaktuar

1.4 Raste praktike

1.4.1 Alice Corporation & CLS Bank International

Fakte dhe rrethana : Alice Corporation është një kompani australiane e cila zotëron patentat '479,'510,'720,dhe '375 të cilat të gjitha kanë të bëjnë me një platformë të kompjuterizuar tregtare që merret me transanksionet financiare në të cilat një palë e tretë zgjidh detyrimet ndërmjet dy të tjera në mënyrë që shlyerja të eleminojnë rrezikun .Rreziku i shlyerjes është rreziku për secilën palë në një këmbim që vetëm njëra palë do të paguajë detyrimin e saj.Patentat e kompanisë Alice e adresojnë këtë rrezik duke përdorur palën e tretë si garantuese.Në 2007 CLS Bank International paditi Alice ku kërkon vendim deklarativ dhe pavlefshmëri të patentave .

5 Neni 17Ligjit nr 9947 datë 7/7/2008 "Për pronësinë industriale"

6 Neni 33Ligjit nr 9947 datë 7/7/2008 " Për pronësinë industriale "

7 Neni 55 po aty

8 Neni 65 po aty

Baza ligjore: Ligji i patentave i SHBA .

Vendimi i gjykatës : Gjykata e SHBA vendosi që patenta e Alice të ishin të pavlefshme pasi në vetvete përmbanin qëllime abstrakte .Kjo është një metodë e të bërit biznes nuk duhet të jetë i patentueshëm .Gjykatat kanë argumentuar gjithashtu pretendimet e Alice nuk kërkon më shumë se një kompjuter gjenerik për të zbatuar këtë ide abstrakte të zgjidhjes së ndërmjetme duke kryer funksione të përgjithshme kompjuterike ,gjë që nuk mjafton për të transformuar një ide abstrakte në një shpikje të pranueshme për patentë .

1.4.2 Rasti i skulptorëve të monumentit Skëndërbeu .

Fakte dhe rrethana : Skulptorët OP,AM dhe JP janë bashkëautorë monumentit të Skëndërbeut e vendosur pranë sheshit Skënderbej. Pretedimet e bashkëautorëve kanë në fokusin e tyre se Banka Tirana Sh.a ka përdorur fotografinë e kësaj vepre për qëllime promocionale si në rrugën drejt aeroportit "Nënë Tereza"Rinas ashtu edhe në ambientet e brendshme të tij pa marrë lejen për shfrytëzimin e saj . Bashkëautorët kërkojnë shpërblimin e dëmit . Gjithashtu kemi 2 vendime të gjykatës civile dhe apelit të rrëzuara për këtë rast. Rekursi nuk është pranuar në gjykatën e lartë.Pretendimet e trashëgimtares së OP kanë të bëjnë me cënimin e aksesit në gjykimin e çështjes ,paanshmëria e vendimit gjyqësor ,cënimi i pronës private duke u bazuar në nenin 1 të protokollit të KEDNJ.

Baza ligjore : 131/f dhe 134/1/I të kushtetutës ,neni 1 Protokolli i KEDNJ

Vendimi gjyqësor : Gjykata kushtetuese nga vetë natyra e saj nuk mund të pranojë çështje të çfarëdo matyre . Ajo është gjykatë ligji dhe jo gjykatë fakti dhe si e tillë e shikon çështjen në aspektin kushtetues nëse janë plotësuar të drejtat të buruara nga kushtetuta apo jo . Gjykata kushtetuese do të ndërhyjë atëherë kur ka cënim për një proces të rregullt ligjor .Detyra e saj është të identifikojë problematika të natyrës kushtetuese dhe jo të zgjidhë mosmarrëveshjen si një gjykatë e shkallës së parë ose si gjykatë apeli . Madje edhe përsa i përket pretendimeve për cënim të së drejtës së autorit po ka cënim të së drejtës së autorit ,por gjykata kushtetuese nuk është kompetente pasi kjo ka të bëjë me analizimin e provave gjë që e ka për detyrë gjykatat e juridiksionit të zakonshëm .

II Ndikimi i krimeve të teknologjisë së lartë tek pronësia intelektuale dhe industriale

2.1 Kriminaliteti kompjuterik, si një dukuri në zhvillim.

Kriminaliteti kompjuterik ka pushtuar botën dhe ka lindur nevoja për specializimin e personave përkatës për t'u marrë me krimet kompjuterike .Për të studiuar një skenë krimi dixhitale është shumë herë me e vështirë pasi potenciali për të gabuar në përfaqësimin e të dhënave është unik për skenat dixhitalë dhe si e tillë hetuesit duhet të marrin masa të posaçme duke marrë parasysh krahasimin e rezultateve të mjeteve të shumta dhe inspektimin e të dhënave duke arritur deri në vërtetësinë e informacionit .Hetuesit dixhitalë kanë arritur deri aty sa të gjejnë edhe informacione të karakterit personal .Përsa i përket juridiksionit në krimet kibernetike është e vështirë pasi aktet e nxjerra në një shtet konsiderohen të ligjshme ,por ama në një shtet tjetër nuk mund të konsiderohet e ligjshme.9Përpara se të hetojmë krimin kompjuterik duhet të kemi parasysh përdorimin e tij dhe njohjen e programeve kompjuterike e-commerce ,e-mail,e-security si dhe programeve të posaçme .Krijimi i programeve solli një evolucion lidhur me identifikimin e transanksioneve rutinë përmes kompjuterit .Aspekt i prekshëm përfshin harduerin,printimet ,disketat .Ndërsa aspektet e paprekshmë përfshin kodin kompjuterik të dhënat dhe informacionin dhe manipulimi i të dhënave brenda kompjuterit .Trendet e krimit kompjuterik kanë të bëjnë me përhapjen e viruseve dhe akteve të tjera sadiste përmes internetit,rritja e sulmeve kundër faqeve të korporatave dhe qeverive me qëllim të vjedhjes së informacionit dhe dhe rritja e vazhdueshme e numrit "hakerave"të rinj dhe agresivë.Shumë sulme kibernetike janë anashkaluar nga autoritetet hetimore dhe pyetja lind kush do t'i hetojë krimet kompjuterikedhe në çfarë niveli?

2.2 Siguria kompjuterike, Kodi penal shqiptar përballë kodeve penale ndërkombëtare.

Siguria kompjuterike ka ndryshuar nga viti në vit ku shqetësimet e sigurisë vinin nga thyerjet fizike vjedhjen e pajisjeve kompjuterike dhe vjedhjen dhe shkatërrimin fizik të paketave të disqeve mbështjellësve të shiritit .Shumë pak njerëz dini të përdornin kompjuterin ku me kalimin e kohës kemi programe të shumëfishta rrjetëzimi dhe ndryshuan rregullat e lojës. Në mënyrë të pashmangshme rritja e disponueshmërisë së sistemeve të informacionit online çoi në abuzim ku kemi ndërhyrjet e personave të paautorizuar për

9 Carl J Franklin "The Investigator's guide to Computer Crime" Library of congress cataloging Springfield Illinois USA 2006

të ndërhyrë në objekte dhe në pajisje kompjuterike dhe shpesh herë sulmet mund të realizohen përmes linjave telefonike dhe informacionit .Nevoja për të ndarë informacione të dhëna të ndryshme aplikacione bën që të kemi një sistem të hapur dhë cënimi i pronësisë intelektuale apo industriale të jetë më i efekshëm.Jemi ende mbrapa që individët ta bëjnë sigurinë pjesë përbërëse të punës së tyre .10Në kodin penal shqiptar dhe jo vetëm krimet kompjuterike dhe siguria e tyre ka qenë prioritet.Shqipëria ka ratifikuar konventën për krimin e fushën e kibernetikës duke e bërë pjesë e së drejtës së brendshme të saj duke filluar tek mashtrimi kompjuterik e cila bëhet me futjen ,fshirjen dhe heqjen e të dhënave kompjuterike me falsifikimin kompjuterik e cila realizohet nëpërmjet futjes së të dhënave apo ndryshimi i tyre me të dhëna të rreme subjektet janë të posaçme pasi ata kanë njohuri specifike lidhur me të. Hyrjet e paautorizuara është një problematikë në Shqipëri pasi shumë vepra arti ,letrare fotografi etj janë përdorur për qëllime për të fituar më tepër të ardhura .Edhe prokuroria bën të mundur ruajtjen e sistemit kompjuterik që këto të dhëna të mos dëmtohen të mos fshihen duke urdhëruar detyrimin për paraqitjen e të dhënave kompjuterike,sekuestrimin e tyre ,ruajtjen dhe mirëmbajtjen e të dhëave kompjuterike.Shqipëria ka marrë modele nga shumë vende të BE dhe janë bërë pjesë e saj,por problematikë ka mbetur eficenca,cilësia dhe efektiviteti i zbatimit të ligjit .

Përfundimet

- Autorët dhe shpikësit kanë të drejta të rëndësishme duke filluar që nga e drejta e mbrojtjes së veprës së tyre, e drejta morale por edhe e drejta ekonomike ka një rëndësi të veçantë .
- Detyrime autorët dhe shpikësit kanë ndaj botuesve dhe organizatave që ata bëjnë pjesë por edhe shtetit për pagesa të tarifave të detyrueshme institucionale
- Shqipëria ka bërë hapa përpara për mbrojtjen e pronësisë intelektuale dhe industriale, por zbatueshmëria e legjislacionit penal dhe të fushave specifike dhe efektiviteti i masave mungon.
- Kriminaliteti kompjuterik ka kapur çdo qelizë tonën duke na monitorituar dhe duke u aksesuar në mënyrë të paautorizuar duke u bërë pjesë dhe e sulmeve kibernetike.
- Mbrojtja ligjore duhet të jetë prioritet i çdo qeverie për të mbrojtur

10 Legjislacioni për krimin kibernetik i ndryshuar Pjesë nga Kodi Penal Ligji Nr. 7895, Datë 27.1.1995 “Kodi Penal i republikës së Shqipërisë ”i ndryshuar .

autorin e veprës & shpikësin në mënyrë që ta motivojë për të punuar më shumë.

- Mbrojtja nga konkurrenca e pandershme ngelet problem në vendin tonë pasi shumë tregtar abuzojnë me çmimet, por edhe me cilësinë e produktit .Madje problematikë në ditët e sotme është që në mallra produktet nuk përkthehen në gjuhën shqipe duke shkaktuar konfuzion dhe mos informimin për pasojat e këtij produkti.
- Siguria kompjuterike sa vjen dhe po avancon dhe e bën më shqetësuese aksesin tonë në inter net duke u ndjerë të rrezikuar kryesisht fëmijët pasi nuk e kuptojnë rrezikun e këtij veprimi. Reklamat e ndryshme për produkte të ndryshme bëjnë që shumë individë të mashtrohen dhe si rrjedhojë mos të marrin produktin në përmasat që ata e kërkojnë.
- Kodi Penal shqiptar është paralel me Kodin penal ndërkombëtar.

Rekomandimet

- Gjykatat shqiptare kanë nevojë për krijimin e seksionit të ri në fushën e pronësisë intelektuale dhe industriale dhe rritet nevoja për ekspertë në këtë fushë .
- Shteti duhet të kontribojë në trajnimin e studentëve dhe ekspertëve në këtë fushë.
- Duhet të garantohen filtra për mbrojtjen e veprave të autorëve dhe shpikjeve apo nxjerrjen e një produkti të tillë në treg .
- Produktet duhet të jenë efektive dhe të jenë me pak kosto për konsumatorin .
- Nëse shpikja në vetvete ka në përbërje lëndë djegëse duhet të bëhën me burime të rinovueshme për të mbrojtur shëndetin tonë dhe mjedisin në tërësi.
- Shqipëria ka nevojë për hetues profesioniste dixhitalë për të hetuar në mënyrë profesionale krimin kibernetik dhe institucionet përkatëse duhet të sigurojnë jetën e individit por edhe veprat e tij
- Zbatimi i legjislacionit kombëtar dhe direktivave të BE do t'i sjellë vendin tonë më shumë siguri dhe stabilitet në rajon.
- Shqipëria duhet të përballet me problematikën kryesore lidhur me konkurrencën e pandershme pasi do të sjelli si pasojë uljen e

investimeve në sektorë strategjikë mbi të gjitha do të humbasë besimi në botimin e veprave letrare ,artistike,shkencore ,muzikore dhe të shpikjeve që do të sjellin zhvillim në vendin tonë.

ALBANIAN CRIMINAL CODE AND PROTECTION OF VICTIMS OF TECHNOLOGY BY VIRTUAL CHALLENGES

ASSOC. PROF. DR. ERVIN KARAMUÇO

Department of Criminal Law Faculty of Law University of Tirana

+355682074556

ervin.karamuco@fdut.edu.al

www.fdut.edu.al

Abstract:

Due to several victims reported recently, caused by virtual challenges mostly in social network such as TikTok, Albania is facing troubles in legal and institutional preventing issues. Absence of specific article in Criminal Law to react with proper measures to condemn the perpetrators is very necessary. Cybercrime law enforcement agencies have serious challenges regarding efforts to combat this phenomenon, due to lack human resources and logistic. Investigators are having many difficulties to identify and prevent these criminal acts, which are committed via virtual accounts, shared in several groups, sometimes in secret, threatening life and abusing vulnerable persons, especially young children.

Regarding danger in young children and teenagers, this kind of criminal activities has been reported continuously with high level of concern by media outlets. The public opinion has denounced the fear and unsecure situation which had jeopardize other human life. During the second half of 2021, according to media reports and official statements of the State Police, 2 young children lost their lives attempting to fulfill the rituals instructed in social networks by mysterious or unidentified accounts. By the end of 2022, Albania has planning to adopt new criminal code and this new legislation is very important to prevent and punishes such dangerous virtual challenges.

This paper aims to analyze the situation of several casualties linked with virtual social account network technology and to reveal adequate reactions and reforms that Albania needs to follow up in order to combat this criminal activity. This paper aims also to realize and identify the dangers caused by virtual challenges crimes, their main causes in the Albanian and the measures that must be taken to prevent them in the future. Another issue taking place in this paper are the adequate proposals for the upcoming articles of new Criminal Code of Albania and the increase of awareness lawmakers and professionals in this field.

Keywords: *technology, criminal code, virtual challenges, social network;*

1. Virtual challenges threats worldwide

Social networks have become a way of life and entertainment for the socialization of many teenagers and young people in our country. According to some authors[1] social media has been linked with several health impacts, particularly in adolescents. More frequent daily social media site visits have been associated with higher odds of depression among individuals between the ages of 12 and 32, and corresponding findings have been reported internationally. Participating in social media becomes a risk to adolescents more often than most adults and risks are seeing in lack of understanding of online dangerous influences.

Addiction to social media is a problem that has created many health and social problems for young people. Cyber bullying has been seen as mechanism used in social media to embarrassing, or hostile information about another person and it is the most frequent online risk for all teenager. In addition to the exchange of information, group chats and various youth trend forums, what has been noticed in recent years is the new trend for challenges between them. These challenges are reported to take place in a form of competition where the one who outdoes the other gets more clicks and sympathy from the group.

Analysts at Bernstein Research Group[2] compared video social network TikTok to a real-life drug addiction, warning of a "digital epidemic" as competition grows in the tech sector. In their report they wrote that TikTok has replaced the user's hesitation about what they want to see, with a bunch

1 Lin, L. Y., Sidani, J. E., Shensa, A., Radovic, A., Miller, E., Colditz, J. B.,& Primack, B. A. (2016). Association between social media use and depression among US young adults. *Depression and anxiety*,

2 https://www.bernsteinresearch.com/brweb/Public/Login.aspx?ReturnUrl=%2fbrweb%2fHome.aspx

of short videos that are managed by a powerful Chinese algorithm. According to this study, the algorithm delivers the most viral content to users, similar to the hormonal rush of drugs, with each swipe.

The Stanford University[3] research reported also that cocaine takes some time to take effect, while more lethal drugs like 'crack' produce their effect immediately, so even though the effect may wear off more quickly, the user is quickly looking for 'another dose,'", which laid out how modern business works, which, like in other sectors, requires the complete and rapid exhaustion of each client's resources, as long as he is 'usable'. This behavior is also seen on other platforms that compete with TikTok, which also aim to turn the network into a "digital crack epidemic."

TikTok social media has been downloaded in about 2 billion subscribers worldwide and still does not have a strict policy to control the age of users. The company in question, like other companies in this field, is interested in expanding its business through clicks, algorithms, advertisements and challenges that become very viral and gain attention and popularity. Many countries have been alerted by the addiction and serious threats from the uncontrolled use of these social media, but still have not found a solution to control the safety of users around the world.

2. TikTok most deadliest challenges

Blackout Challenge, also known as the "choking game" or "fainting game," directs users to cut off their air supply by choking themselves until they pass out. This game propagandizes to the users the idea of the burst of adrenaline the moment you wake up after faint and understand how important life and sacrifice are to stay alive. This game is believed to be the deadliest act used by teenagers all over the world by TikTok. Currently, in countries such as America, England and Italy, there are dozens of cases where parents have filed lawsuits against TikTok regarding the loss of their children's lives.

Benadryl Challenge is a social media trend in which teens are encouraged to ingest higher than recommended doses of the over-the-counter allergy medicine diphenhydramine (Benadryl) in order to achieve a "high." Teens may perceive the over-the-counter drug to be relatively safe, and therefore, participate in the challenge. Typical presentations are unexplained drowsiness, disorientation, or hallucinations, often associated with pupillary dilatation. The level of consciousness typically ranges from coma to delirium. Other symptoms include dry mouth, blurred vision, and urinary retention. Seizures

3 https://scopeblog.stanford.edu/2021/10/29/addictive-potential-of-social-media-explained/

and cardiac arrest are possible, in common with other anticholinergic drugs[4].

Skull Breaker Challenge, is already very danger widespread challenge between groups which leads in potential fatality. It involves people, usually three, jumping next to each other, and two of them kick out the third's feet from under them, causing them to fall backwards on their head. The viral trend has been reported causing injuries across US high schools. Health experts have condemned this challenge for its propensity to cause "serious and life-threatening injuries" like skull-fracture, paralysis or even death[5].

The Fire Challenge leads the teens to cover their body in an inflammable substance and then light it on fire. Despite its obvious dangers, this challenge found several takers among unassuming 12 and 13-year-olds. This resulted in a number of children being hospitalized for first and second-degree burns in US. In addition to the obvious dangers, many participants run away in panic without dousing the flames first, allowing the oxygen to cause the flames to spread more easily. Another immediate danger is the participants inhaling superheated air, which can then damage the lungs[6].

Hot water challenge, has involved behavior drinking boiling water to reach others quantity. This act can cause serious injury and reportedly led to the deaths of several peoples. The new version shown on TikTok involves dumping boiling water on oneself or friends causing first and second degree burns on the body. This is very danger because, young kids might find this dare "cool" or "fun", but may not understand that pouring boiling hot water on someone causes serious irreparable damage and even possibly death[7].

Blue Whale Challenge has the potential to be the deadliest consequences. According to the studies, this challenge poses real danger, given the fickle nature of teenagers. While many continue to believe that it's little more than an online hoax, the potential for death is too high to write this challenge off[8]. The Blue Whale Challenge is a suicide challenge, which introduces participants with 50 tasks, all of which must be undertaken over the course of 50 days. Many of the included duties are innocent enough, but the final request is always the same, and if heeded will always result in death. The challenge has unfortunately endured for years despite its grim requirements

4 https://bcmj.org/blog/tiktok-benadryl-challenge-alert-physicians

5 https://www.health.com/mind-body/skull-breaker-challenge-tiktok

6 http://www.nbcmiami.com/news/local/Fla-Kid-Suffers-2nd--3rd-Degree-Burns-from-Fire-Challenge-269481181.html

7 https://injury.research.chop.edu/blog/posts/hot-water-challenge

8 https://icpalazzolo.edu.it/wp-content/uploads/sites/90/Vademecum-su-Blue-Whale-Challenge.pdf

and continues to spark major concern amongst parents[9].

3. TikTok casualties in Albania

Albania, like other countries, due to the increased use of social networks, has not remained unaffected by the dangers of online challenges. Within a few years, there has been information, especially in schools, of the increased interest of children and teenagers to participate in various rituals on the internet that were related to certain challenges. Through these networks, they feel good to follow the trend of other friends, to accept the status as a way to be accepted by the group, as well as an opportunity to avoid being bullied or excluded from society.

As a result of the uncontrolled increase in use of the internet by children and teenager, out of family, society or school attention, and in the total lack of interest of institutional strategy and propaganda, within the last 6 months of 2021, 2 children have been reported dead in Albania due to TikTok Blackout challenge.

The first event happened in June 2021 in the city of Shkoder, where a 10-year-old child lost his life while making a video on TikTok. The 10-year-old started making the video when he was alone at home, but something went wrong, ending in tragedy. According to the police, his parents found him when they returned home a few hours later. When police forces arrived at the scene, preliminary investigations have revealed the challenge that the child was making. He was riding on a bench and had the rope around his neck, but the bench moved and the minor was left hanging, apparently without a chance to escape[10].

Another casualty occurred on November 2021, when 13-year-old died after hanging himself with a rope around his neck in his room in city of Lushnje. He was found dead by his parents, where even though he was taken to the hospital, it was too late for him. The police started investigation and then clarify that the reasons that have led the minor to hang himself where linked with the video on the TikTok social network. These have been confirmed by the police, after 13-year-old's friends testify that the minor frequented social networks and liked TikTok challenges[11].

Another profile of the above victim was made by other classmates and his TikTok account where the young man shared images of depression, violence

9 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6009009/

10 https://kohajone.com/10-vjecari-vdes-ne-menyre-tragjike-teksa-po-realizonte-video-per-tiktok/

11 https://dosja.al/e-rende-13-vjecari-ne-lushnje-po-bente-video-per-tik-tok-shokunuk-preu-dot-spangon

and loneliness. His profile is called 'Bad boy', while his writings showed a state of heavy depression and also very lonely. The last testimony had shown that the teenager was a user of social networks and his death is related to the making of a video. One of them told the authority that 13-year-old's friends planed before to get on the chair, tied a rope around his neck and let go of the chair. According to him, the knife failed to cut the string tied[12].

Both of the above cases resulting in the death of children have in common the almost identical nature of the challenge ritual in TikTok. The testimonies of the victims' families and friends show that their closed nature, depression, despair and boredom were the reasons they choose to try dangerous things, as part of their incentive to feel good. The problem faced by society and institutions is related to the fact that the age of children does not really understand the danger of these challenges. This makes them fall into a virtual trap, from which they have a very high probability of becoming victims.

4. Legal framework and administrative action to prevent TikTok challenges casualties

In the above two cases, regardless of the investigations and their results by the police, the prosecutor's office initially filed charges for causing suicide, but later both cases were dismissed due to the lack of further evidence to accuse specific persons. According to Criminal Code of Albania[13], causing suicide or attempted suicide of a person, as a result of systematic ill-treatment or other systematic behavior that seriously affects dignity, committed by the person who depends on him or by the person with whom he has a family or cohabitation relationship, is sentenced to imprisonment from three to seven years.

Analyzing the above provision, it is noticeable that its content does not foresee cases where the cause of suicide may come from certain networks or technologies that promote, share, provide and distribute dangerous challenges to life and health. Furthermore, the Criminal Code in force does not provide for other articles to provide the prevention and punishment of such cases among children from the side of applications and social networks.

In the case of information technology corporations that offer online service networks, Albanian law[14] provides criminal liability. In cases of committing criminal offenses, based on this law, legal entities face fines

12 https://www.report-tv.al/lajm/vetevaret-nje-13vjecar-ne-lushnje-dyshohet-se-po-bente-video-ne-tiktok

13 Article 99 of Criminal Code of Albania

14 LAW No. 9754, dated 14.6.2007 ON CRIMINAL LIABILITY OF LEGAL PERSONS

or deregistration and termination of their activity. These punishments are related to specific offenses provided in criminal code. In cases where the criminal code does not provide specific acts committed by these entities, such as the case of social network companies, then this law is impossible to apply as a punitive measure in the context of a criminal process to find responsibility for causing the suicide of children or the serious risk of their lives.

The only legal way that can be followed currently in the Republic of Albania for measures against pages or accounts on the internet that seriously endanger life and health is to appeal to the court or to file charges in prosecutor office for the damage caused and dangers by illegal and hazard online games and challenges. The authority than might ask the Electronic and Postal Communication Agency to start procedures with internet service providers in Albania to restrict access to a number of websites, including online blogging platform[15]. The issue that requires a proper legal interpretation to set the authorities in motion is the legal basis for arguing the danger to life from online challenges and the elements of illegality that these sites or programs present according to Albanian law. In this aspect, as I mentioned above, there is again the possibility to deal with a legal vacuum of a criminal nature and lack of technical regulations in this field of electronic communications technology.

Another issue that requires attention and special institutional focus is education and propaganda in schools and other educational institutions on the prevention of models that children follow and those who need to be involved in online challenges. Despite the promises of the Ministry of Education[16] for the opening of a public debate on this issue and the drafting of a defense strategy from information technology, there is still no special official document to determine the rules and concrete action plan in this field. The vacuum in the aspect of institutional initiatives is another shortcoming that allows an uncontrolled field of action of the dangerous activity of using digital accounts and programs on sites that contain dangerous games for children.

5. Conclusion

The uncontrolled use of social networks and online challenges that endanger the life and health of minors continues to be quite disturbing and

15 LAW No. 9918, dated 19.5.2008 FOR ELECTRONIC COMMUNICATIONS IN THE REPUBLIC OF ALBANIA (amended by law no. 102/2012, dated 24.10.2012, no. 107/2018, dated 20.12.2018; no. 92/2019, date 18.12.2019)

16 https://albaniandailynews.com/news/13-year-old-dies-trying-to-do-a-video-for-tik-tok-minister-reacts-

without a concrete legal and institutional preventive measure.

An amendment to the current legislation is needed to define in clear and concrete terms the type of technological attacks on the life and health of children and adolescents, criminal penalties and other administrative measures against the social networks involved.

Institutions of social services, education and schools, must draw up a strategic plan of immediate action to propagate measures to prevent the dangerous use of social networks, by launching ongoing public awareness campaigns.

The independent institutions that supervise social networks and internet providers in Albania, must take initiatives to intervene with decisions in every case when data is reported for abuse of internet accounts which threat the life and health of children and teenagers.

Through public funding, the media and other sources of information on the Internet should undertake a civil initiative to denounce the danger of TikTok challenges, promoting new rules and behaviors to prevent the loss of children's lives in the future.

It is very imperative that special instructions of controlled parental monitoring be made public to be followed as models by those families who have an increased risk of facing dangerous actions of their children included in the Internet network where the TikTok challenges are applied.

6. Bibliography

Law No .7895, datë 27.1.1995 (amended) Criminal Code of Albania

LAW No. 9754, dated 14.6.2007 ON CRIMINAL LIABILITY OF LEGAL PERSONS

LAW No. 9918, dated 19.5.2008 FOR ELECTRONIC COMMUNICATIONS IN THE REPUBLIC OF ALBANIA (amended by law no. 102/2012, dated 24.10.2012, no. 107/2018, dated 20.12.2018; no. 92/2019, date 18.12.2019)

Lin, L. Y., Sidani, J. E., Shensa, A., Radovic, A., Miller, E., Colditz, J. B.,& Primack, B. A. (2016). Association between social media use and depression among US young adults. *Depression and anxiety*,

https://albaniandailynews.com/news/13-year-old-dies-trying-to-do-a-video-for-tik-tok-minister-reacts-

https://kohajone.com/10-vjecari-vdes-ne-menyre-tragjike-teksa-po-

realizonte-video-per-tiktok/

https://dosja.al/e-rende-13-vjecari-ne-lushnje-po-bente-video-per-tiktok-shokunuk-preu-dot-spangon

https://www.report-tv.al/lajm/vetevaret-nje-13vjecar-ne-lushnje-dyshohet-se-po-bente-video-ne-tiktok

https://injury.research.chop.edu/blog/posts/hot-water-challenge

https://icpalazzolo.edu.it/wp-content/uploads/sites/90/Vademecum-su-Blue-Whale-Challenge.pdf

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6009009/

https://bcmj.org/blog/tiktok-benadryl-challenge-alert-physicians

https://www.health.com/mind-body/skull-breaker-challenge-tiktok

http://www.nbcmiami.com/news/local/Fla-Kid-Suffers-2nd--3rd-Degree-Burns-from-Fire-Challenge-269481181.html

https://www.bernsteinresearch.com/brweb/Public/Login.aspx?ReturnUrl=%2fbrweb%2 fHome.aspx

https://scopeblog.stanford.edu/2021/10/29/addictive-potential-of-social-media-explained/

PASTRIMI I PRODUKTEVE TË VEPRËS PENALE OSE VEPRIMTARISË KRIMINALE ÇËSHTJE TË PRAKTIKËS GJYQËSORE

MIGENA LASKA

Gjykata e Rrethit Gjyqësor Tiranë

Dhoma Penale

migenachris@yahoo.com

I. HYRJE

Në kuptim të nevojës aktuale të zhvillimit dhe intensifikimit sikurse edhe të sofistikimit të masave ligjore, proçedurale si dhe gjyqësore, për të luftuar dhe eliminuar, o në mos për të minimizuar zhvillimin e veprimtarive me karakter kriminal, për shkak të aktivitetit jo vetëm keq bërës, por edhe fitim prurës në sasi të konsiderueshme, brenda një kohe të shkurtër, si dhe mbi të gjitha në mënyrë të paligjshme e të pajustifikuar, lind domosdoshmëria e një trajtimi doktrinal por edhe konkret (ilustrues), duke e qasur dhe krahasuar infrastrukturën ligjore vendase dhe të huaj, krahas praktikës gjyqësore, e duke analizuar në mënyrë të hollësishme elementët përbërës dhe prezentë të figurës së një vepre penale, të re për legjislacionin shqiptar, jo shumë të lëvruar në praktikat gjyqësore, por shumë të ndjeshme dhe të prekur në përditshmërinë e proçedimeve penale, të cilat në veçanti lidhen me ndjekjen penale kundër veprave apo veprimtarive kriminale, të cilat në vetvehte lidhen kryesisht me krimin e organizuar, organizatat kriminale, trafikun e armëve, qënieve njerëzore, lëndëve narkotike, ushtrim apo shfrytëzim prostitucioni, korrupsioni.

Ky është në mënyrë shumë sistetike fokusi i këtij trajtimi teorik, duke u përqëndruar posaçërisht tek figura e veprës penale të "***Pastrimi i Produkteve të Veprës Penale apo të Veprimtarisë Kriminale***", e parashikuar nga neni **287 i Kodit Penal Shqiptar**.

II. HISTORIKU

Para viteve 1990 termi "***pastrim parash***", nuk përdorej dhe nuk njihej nga shoqëria shqiptare. Kjo dukuri kriminale është relativisht e re (*veçanërisht për vendin tonë*) dhe lidhet në vetvehte si dhe vjen si produkt apo pasojë e një aktiviteti kriminal, të kryer në kuadër të krimit të organizuar.

Në legjislacion penal shqiptar, kjo vepër njihej (më parë) me formulimin "***Tjetërsimi dhe fshehja e pasurisë***" që parashikohej ne nenin 287 i Kodit Penal të Republikës së Shqiperisë.

Për herë të parë në legjislacionin tonë penal, "***Pastrimi i parave të pista***", u parashikua, në vitin 2000, me hyrjen në fuqi të ligjit nr. 8610, date 17.05.2000, i cili në nenin 2 të tij parashikonte: "***Pastrimi i parave është qarkullimi dhe riqarkullimi i parave të rrjedhura nga veprimtaria kriminale"***.

Azhornimet ligjore, të ndërmarra ndwr vite (*2000, 2003, 2007, 2012, 2021*) për përcaktimin dhe rregullimin ligjor të kësaj vepre penale patën rëndësi për kohën, duke mbajtur një qëndrim të qartë ndaj kësaj dukurie kriminale të sapo shfaqur.

Termi "*pastrim i parave*" (*Money Laundering*), për herë të parë është perdorur në **SHBA në vitet 70-80.**

Shfaqja e një dukurie të tillë erdhi si pasojë e rritjes së të ardhurave të grupeve kriminale nga tregtia e paligjshme e lëndëve narkotike dhe më pas ri investimi i këtyre të ardhurave të paligjshme në ekonominë e ligjshme amerikane.

Kjo dukuri u emërtua si transformim i parave të pista, të përfituara në rrugë të paligjshme, që kishin prejardhje të pa-ligjshme, dhe që hynin më pas në qarkullimin monetar.

Ky kërcënim serioz global, u vlerësua fillimisht si i tillë në SHBA, ku dhe nisi angazhimi luftën e organizuar kundër këtij fenomeni kriminal dhe që rrezikon rendin juridiko shoqëror dhe ekonomik në rrafsh global.

Kështu, në fillimet e viteve '80, ***Komiteti i Bazelit***, që përbëhej nga përfaqësuesit e bankave angleze, belge, gjermane, italiane, kanadeze, amerikane, franceze, zvicerane dhe japoneze, e shqyrtuan këtë problem në nivel ndërkombëtar, në vitin **1988** mbasi analizoi gjëndjen e krijuar, doli me deklaratën e njohur "*Për ndalimin e përdorimit të sistemeve bankare për qëllime të larjes së parave të ardhura nëpërmjet rrugëve kriminale*".

Në vijim janë hartuar dhe miratuar aktet ndërkombëtare si më poshtë:

1. *Rekomandime per parandalimin nga sistemet bankare te larjes se parave", 1988. rekomandime për zbatimin e një sërë masash e rregullash në sistemet bankare si dhe evidentuan kërkesen për organizimin e luftës kundër kësaj dukurie ku merrnin përparësi metodat e kontrollit të operacioneve për të gjitha transfertat bankare.*
2. *Në vitin 1989, anëtarët e shtatëshes (G7) krijuan grupin e veprimeve ndërkombëtare të quajtur: Grupi Ndërkombetar i Veprimeve Financiare (Groupe D'Action Finansiere International, GAFI), i përbërë nga përfaqësues te shteteve pothuaj nga e gjithë bota.*
3. *Në vitin 1990 ky organizëm publikoi një program special masash për luften kundër "larjes së parave të pista", në të cilin jepen mbi 40 rekomandime, të pranuara dhe të vëna në zbatim nga shumë shtete të botës.*
4. *Konventën e Vjenës e OKB-se "**Kundër krimit të organizuar ndërkombëtar**", 15 nëntor 2000,*
5. *Komiteti i Bazelit "**Për kontrollin e sistemeve bankare**",*
6. *Konventa e kombeve të Bashkuara kundër trafikut të paligjshëm të drogave Vjenë, 1998 parashikon që sekreti bankar nuk mund të përdoret asnjëherë për të refuzuar bashkëpunim për sa u përket fitimeve që vijnë nga veprat penale të lidhura me drogën ose pastrimin e parave.*
7. *Konventa Ndërkombëtare e Luftës kundër Financimit të Terrorizmit e Kombeve të Bashkuara 1999, punimet e grupit të veprimit financiar për pastrimin e kapitaleve (GAFI),*
8. *Rezoluta 1373 (2001) mbi kercenimin e paqes dhe siguris nderkombetare qe vjen nga aktet terroriste, e miratuar nga Këshilli i Sigurisë i OKB-se me 28 shtator 2001;*
9. *Konventa mbi pastrimin e Parave, Zbulimin, Kapjen dhe Konfiskimin e Pasurive të vëna me anë të krimit dhe mbi Financimin e Terrorizmit (2005);*
10. *Direktiva 91/308/CEE e 10 qershorit 1991, e ndryshuar me 4 dhjetor 2001, dhe së fundi dy vendimet e Bashkimit Europian, të datës 26 qershori 2001 dhe 24 shkurtit 2005.*

11. *Konventa e Varshavës, në datë 16 maj 2005 për "Pastrimin e parave, zbulimin, kapjen dhe konfiskimin e pasurive te krimit dhe financimin e terrorizmit". 2.1 Financimi i terrorizmit.*

Sipas nenit 2 te Konventës së Varshavës, se vitit 2005, secili shtet miraton ligjet e nevojshme për trajtimin e financimit të terrorizmit sipas rregullave të treguara në kapitullin III (masat qe duhen marrë në nivel kombëtar), në kapitullin IV (bashkepunimi nderkombetar) dhe në kapitullin V (bashkëpunimi mes njësive të shërbimeve të fshehta financiare). 2.2 Masat që duhen marrë në nivel kombetër.

Krahasimisht me Konventën e vitit 1990, vjen si risi detyrimi për vendet nënshkruese të shpallin financimin e terrorizmit si vepër penale.

12. *G7 ka miratuar 40 rekomandime për luftën kundër pastrimit të parave, shiko B. Bouloc, La prevention du blanchiment d'argent, Rev. dr.bancaire et financier, 2002, nr. 6, f. 359, dhe nga i njëjti autor De quelques aspects du delit de blanchiment, id. 2002,nr.3,f, 15 I".*

III. QËLLIMI I VEPRIMTARISË KRIMINALE

Pastrimi i parave ndjek dy qëllime përfundimtare të paligjshme:

1. ***Të fshehë ekzistencën e veprës penale e cila ka gjeneruar pasuritë kriminale, dhe e cila kryhet për motive të përfitimit ekonomik*** *(p.sh trafiku i drogës, evazioni fiskal, korrupsioni, trafikimi i qënieve njerëzore, trafikimi i armëve, ushtrimi apo shfrytëzimi i prostitucionit, etj si këto)**;***
2. ***T'u mundësojë autorëve të veprës penale t'i "gëzojnë" frytet e veprimtarisë së tyre kriminale, duke i konsumuar apo investuar gradualisht, në forma dhe mënyra nga më të ndryshmet e në ekonominë e ligjshme.***

Për arritjen e këtyre qëllimeve finale kriminale, autorët e veprës penale të "***pastrimit të produkteve të veprës penale/parave***" ndjekin disa qëllime të ndërmjetme si tjetërsimi i pasurive, krijimi i personave juridikë fiktivë, rregjistrimi i pasurive nën emrat e pronarëve të rremë etj.

Për rrjedhojë, analiza juridike e luftës kundër këtij fenomeni të rrezikshëm paraqet disa problematika specifike, dhe nuk kryhet vetëm brenda kuadrit konceptual të së drejtës penale, por brenda një kuadri gjithë përfshirës të politikave publike dhe masave legjislative.

IV. PËRKUFIZIMI I PARAVE TË PISTA

Pastrim i produkteve të veprës penale quhet legalizimi i mjeteve monetare dhe i pasurive të fituara në mënyrë të paligjshme, thënë ndryshe, pastrimi i parave të pista.

Termi "***pastrimi i parave***" nënkupton rastin kur paratë përfaqësojnë frytet/produktet e veprimtarisë kriminale dhe mund të jenë jo vetëm në trajtën e parasë fizike por edhe fonde të cilat mund të përdoren për shlyerjen e një detyrimi monetar (legal tender), apo instrumentat financiare të vlerësuara si të drejta personale/kreditore dhe që mund të konvertohen në tregun financiar në mënyrë likuide në vlera monetare.

Pastrimi i parave është një proçes që në fazën e parë të tij synon të fshehë ekzistencën dhe/ose burimin e paligjshëm të produkteve të veprave penale, dhe në fazën e dytë synon t'i japë pasurive vlerë ligjore.

Ky krim, që parashikohet në legjislacionin penal shqiptar, është një nga format e shfaqjes së krimit të organizuar, të terrorizmit ndërkombëtar dhe korrupsionit.

Për të krijuar një koncept të saktë se çfarë përfaqëson kjo vepër penale në rrafshin kriminologjik, në funksion të krimit të organizuar dhe të korrupsionit, duhet të kemi të qartë se çfarë nënkupton "*legalizimi i mjeteve monetare dhe i pasurive të fituara në rrugë jo ligjore ose pastrimi i parave të pista*".

Thelbi i këtij veprimi kriminal qëndron në synimin e pronarëve të këtyre mjeteve monetare apo pasurive të fituara në rrugë kriminale për të krijuar kushte, nëpërmjet veprimtarisë së kundërligjshme, që t'i gëzojnë ato sikur të ishin përfitime të ligjshme.

Për këtë qëllim ata përdorin mjete dhe metoda nga më të ndryshmet, ku veçohen teknikat e futjes në qarkullim dhe ri-qarkullimin e parave që kanë rrjedhur nga veprimtaria kriminale.

Legalizimi i mjeteve monetare dhe i pasurisë së fituar në rrugë të paligjshme realizohet nëpërmjet veprimeve të tilla, si: *Depozitimi, tjetërsimi, transferimi ose këmbimi i parave me qëllim maskimin, fshehjen ose mohimin e përkatesise apo origjines se pasurise qe rrjedh nga veprimtaria kriminale*.

Një nga kushtet e domosdoshme per realizimin e synimeve kriminale është legjitimimi apo legalizimi i këtyre pasurive me prejardhje kriminale. Në thelb që i bën "***paratë e pista***" të duken të pastra, është veprimtaria kriminale që përfshin përpjekjet për të fshehur ose maskuar të ardhurat kriminale.

V. VËZHGIM I PËRGJITHSHËM MBI "PASTRIMIN E PARAVE"

Pastrimi i parave është proçesi i marrjes së fondeve të siguruara në mënyrë të kundërligjshme dhe duke përdorur transaksione të ndryshme për të krijuar përshtypjen sikur paratë janë të përligjura. Me qëllim gëzimin e tyre sa më të qetë në jetën dhe aktivitetin e tyre të përditshëm, duke përballuar shpenzime nga më të ndryshmet, investime, duke krijuar pasuri (*të luajtshme dhe të paluajtshme*), duke kryer aktivitet ekonomik privat, dhe jo vetëm, etj.

"***Procesi i pastrimit të parave mund të ndahet në tre faza;***

a) depozitimi i parave në institucione financiare,

b) transferimi elektronik në një numër llogarish;

c) integrimi me paratë e pastra.

Faza e parë, e depozitimit të parave në institucione financiare përfaqëson hyrjen fillestare të produkteve të veprës penale në sistemin financiar. Kjo fazë shërben për dy qëllime – ajo e çliron autorin e krimit nga mbajtja dhe ruajtja e vëllimit të madh të parave fizike dhe i vendos paratë në rrjedhën financiare të përligjur. Faza e depozitimit vlerësohet si më e rrezikshmja, sepse në këtë fazë mundësitë e krijimit të dyshimit janë më të mëdha.

Faza e parë e transferimit të vëllimit të parasë fizike produkt i drogave ose krimeve të tjera shpesh përfshin kontrabandën nga një shtet në tjetrin. Shuma e parave fizike që kontrabandohen, sigurisht që vjen në rritje, si pasojë e rregullave që vendosen për të monitoruar paratë fizike të kaluara nëpërmjet institucioneve tregtare dhe financiare.

Depozitimi në institucione financiare, ***transferimet eletronike në një numër llogarish dhe integrimi me paratë e pastra,*** janë terma të drejtë që përshkruajnë një proçes.

Faza e dytë. Pas depozitimit të parave në institucione financiare vjen faza e transferimit elektronik në llogari të ndryshme, që normalisht përbëhet nga një sërë transaksionesh të synuara për të fshehur origjinën e fondeve. Kjo është faza me natyrë më të ndërlikuar dhe më ndërkombëtare. Gjatë kësaj faze, për shembull, pastruesi i parave mund të fillojë me kalimin e fondeve në mënyrë elektronike nga një shtet në tjetrin, pastaj i ndan ato në investime të vendosura në opsione financiare të përparuara ose në tregje të vendeve të tjera, duke i lëvizur ato vazhdimisht për t'iu shmangur zbulimit, duke shfrytëzuar çdo herë të çara ose papajtueshmëri në legjislacion.

Vendet pa legjislacion të përshtatshëm i ndihmojnë pastruesit e parave

duke mos i lejuar hetuesit të gjurmojnë rrjedhën e fondeve të paligjshme nëpërmjet sistemit financiar të tyre.

Faza e tretë, e pastrimit të parave është "***integrimi me paratë e pastra***".

Fondet i rikthehen kriminelit duke krijuar përshtypjen se janë siguruar nga burime të përligjura. Pasi janë depozituar fillimisht si para fizike dhe pasi janë transferuar elektronikisht nëpërmjet një numri operacionesh financiare, produktet kriminale integrohen plotësisht në sistemin financiar dhe mund të përdoren për çdo qëllim, përfshirë financimin e më shumë krimeve.

VI. ELEMENTËT E DISPOZITËS LIGJORE TË VEPRËS PENALE

Kuptimi i elementeve të veprës penale është vendimtar për suksesin e hetimit, deri në zgjidhjen e çështjes bazuar në një vendim gjyqësor të formës së prerë.

Elementi i parë është "***këmbimi ose transferimi i pasurisë***". Në thelb çdo lloj transaksioni financiar në vetvehte e përmban këtë element, përfshirë transaksionet me para fizike, çek bankar, transferim elektronik ose me një objekt të paluajtshëm. Zakonisht ky është elementi më i evidentueshëm për t'u vërtetuar në një rast të pastrimi të parave.

Elementi i dytë kërkon që transaksioni duhet të bëhet me "***produktin e veprës penale***". Dispozita nuk jep një përkufizim konkret të termit "***produkt i veprës penale***". Në shumë raste vërtetimi i këtij elementi mund të jetë i vështirë, por domosdoshmërisht nevojitet që të sigurohen prova të mjaftueshme të cilat përtej dyshimit të arsyeshëm, të bindin Gjykatën, se paratë e përfshira në transaksion e kanë origjinën nga një veprimtari kriminale. Këtu padyshim, nevojitet edhe kryerja e një ***hetimi pasuror të hollësishëm***, sa i takon justifikimit të ligjshëm të burimit të krijimit të pasurisë përkatëse, apo transaksionit përkatës, apo të hollave të evidentuara.
*****

Elementi i tretë përmbush kërkesën ***e dijenisë***, e të paturit dijeni.

Sa i përket këtij elementi, që kërkon dispozita ligjore, nevojitet të provohet, fakti se personi i përfshirë në transaksion kishte dijeni se paratë e kishin origjinën nga "***produkti i veprës penale***". Pra, pasja dijeni se origjina e pasurisë është e paligjshme.

Elementi i katërt, kërkon që transaksioni duhet të bëhet për një qëllim: "***për të mbuluar ose fshehur origjinën e pasurisë***". Shpesh ky element

mund të vërtetohet duke provuar që personi ka përdorur një kompani guaskë ose një person tjetër, për të fshehur burimin e vërtetë të fondeve. Në një rast hipotetik: mund të ndodhë që një person totalin e të ardhurave të krijuara nga veprimtaria e paligjshme/kriminale, e copëzon në disa transaksione të ndara, dhe i depoziton këto shuma në banka të ndryshme, me qëllim që të shmangë detyrimin e raportimit, të parashikuar në ligj.

Shumë trajtime teorike në të drejtën penale ndërkombëtare, sikurse edhe në shumë legjislacione penale, e trajtojnë zgjidhjen e këtij problem në një mënyrë krejt ndryshe.

Pranojnë faktin se, dy veprat penale (***ajo mëmë dhe atë bijë***), ajo kryesore ashtu dhe ajo (bijë) e "***pastrimit të produkteve të veprës penale***", kanë të njëjtin objekt në vetvehte, pra cënojnë të njëjtën mardhënie juridike penale, të njëjtin interes të mbrojtur ligjërisht në mënyrë të posaçme dhe nëse veprimet si element të anës objektive të përshkruara në përkufizimet e tyre janë të ngjashme. Nga doktrina e huaj, është konsideruar se autori i aktit paraprak nuk mund të dënohet edhe për pastrim parash, duke përdorur konceptin e privilegjit, bazuar në privilegjin e vetëfshehjes.

Baza për mos-ndëshkimin e autorit të veprës penale kryesore dhe njëkohësisht edhe për veprën penale të pastrimit është parimi "*ne bis in idem*" (***një vepër një dënim***), që autori i veprës penale nuk mund të detyrohet të dorëzohet para drejtësisë, për fshehje të mallrave që rrjedhin nga vepra e tij.

Në fund, baza për mos-ndëshkimin e vetë-fshehjes është koncepti i aktit të mëvonshëm të bashkë-penalizuar, sepse nuk ka interes të ri të mbrojtur me ligj dhe kriteri që një sjellje e ndryshme nuk mund të jetë e nevojshme, duke respektuar të drejtën e një personi për të mos fajësuar veten. Pra, logjika juridike në disa legjislacione të huaja, qëndron në argumentin se: "vetë-fshehja" shkon pa u ndëshkuar për shkak se ajo është shterimi i vetë veprës penale "mëmë".

Pavarësisht se pastrimi i parave, nga disa legjislacione konsiderohet një formë e fshehjes, rezulton se një ndër elementet themelor të tij është lidhja me krimit organizuar. Sakaq, qëllimi final i kriminalizimit dhe dënimi i veprës penale të pastrimit të parave, është sanksionuar në ligj për të mbrojtur shtetet nga krimi i organizuar dhe veprimtaria e organizatave kriminale, të cilët dëmtojnë seriozisht ekonominë dhe organizuar sipas legjislacionit fiskal të çdo vendi, duke vendosur në kërcënim stabilitetin, sigurinë dhe sovraniteti i shteteve. Sigurisht duke ardhur në kundërshtim me rendin dhe organizimin juridik të një vendi, sistemin e rregullave mbi të cilat një vend është i organizuar dhe funksionon.

Për këtë arsye, ka lindur nevoja dhe domosdoshmëria që fenomeni i pastrimit të parave të trajtohet jo vetëm si një formë e fshehjes së të ardhurave, por edhe si një vepër e veçantë kundër rendit juridik social ekonomik të një vendi. Ndaj dhe është parashikuar në kodin penal si një figurë e veçantë e veprës penale, e cila sanksionon pikërisht këtë fakt penal.

VII. FIGURA E VEPRËS PENALE:

"*Pastrimi i produkteve të veprës penale dhe veprimtarisë kriminale*", parashikuar nga neni 287 të Kodit Penal.

Objekti i kësaj vepre penale përfaqëson tërësinë e marrëdhënieve juridike të vendosura nga ligjvënësi me qëllim garantimin e funksionimit të rregullt dhe normal të organeve të administratës publike dhe mbrojtja e interesit të shtetit dhe shtetasve nga pastrimi i produkteve të veprës penale. Objekti material përfaqëson vetë produktin e veprës penale që pastrohet.

Në lidhje me anën objektive të figurës së veprës penale "***Pastrimi i produkteve të veprës penale ose veprimtarisë kriminale***".

Në lidhje me nocionin "***produktit të veprës penale ose veprimtarisë kriminale***", Neni 1 i Konventës së Këshillit të Evropës "*Për Pastrimin, Kërkimin, Kapjen dhe Konfiskimin e Produkteve të Krimit dhe Për Financimin e Terrorizmit*" jep këtë përkufizim:

"Për qëllime të kësaj Konvente:

*a) "**produkt**" nënkupton çdo avantazh ekonomik të nxjerrë nga veprat penale. Ky avantazh mund të konsistojë në çdo pasuri, siç përcaktohet në nënparagrafin b të këtij neni;*

*b) "**pasuri**" nënkupton pasuri të çdo natyre, fizike ose jofizike, e luajtshme ose e paluajtshme, si dhe aktet juridike ose dokumentet që vërtetojnë një titull ose interes mbi këtë pasuri;".*

Nocionin e "***produktit të veprës penale***" e gjejmë edhe në **nenin 36 të Kodit Penal**, i cili parashikon se:

"1.) Konfiskimi jepet detyrimisht nga gjykata dhe ka të bëjë me marrjen dhe kalimin në favor të shtetit:

a) *të sendeve që kanë shërbyer ose janë caktuar si mjete për kryerjen e veprës penale;*

b) *të produkteve të veprës penale, ku përfshihet çdo lloj pasurie, si dhe dokumentet ose instrumentet ligjore që vërtetojnë tituj ose*

interesa të tjerë në pasurinë që rrjedh ose fitohet drejtpërdrejtë ose tërthorazi nga kryerja e veprës penale;".

VIII. PRAKTIKA GJYQËSORE VENDASE

Me vendimin ***nr. 4, datë 23.02.2011, pika 22 të Gjykatës Kushtetuese***, në përputhje me standartet e Gjykatës Evropiane për të Drejtat e Njeriut, është parashikuar se ***organi i Prokurorisë në çdo rast ka për detyrë që të identifikojë pasuritë të cilat pretendohen se janë produkt i veprimtarisë kriminale*** të parashikuar nga neni 3 i ligjit, me qëllim që interesi publik, i cili determinon në vendosjen e kufizimit të pronës të jetë në proporcion me masën që merret duke u vendosur vetëm mbi ato pasuri të cilat e kanë burimin nga aktiviteti kriminal[1].

Me vendimin Nr. 201 datë 09.12.2015 Kolegji Penal i Gjykatës së Lartë ka arsyetuar:

" Së pari: *prania e elementit të fumus commissis delicti, domethënë që sendi duhet të ketë qenë ai që ka shërbyer apo ai i destinuar për kryerjen e veprës penale, apo se është pikërisht ai që përbën produktin e veprës penale, shpërblimeve, të dhëna, prodhimi, përdorimi, mbajtja ose tjetërsimi i së cilit, përbën veprën penale.*

Së dyti, *është e nevojshme vërtetimi i një lidhjeje të posaçme, funksionale dhe jo të rastësishme (domethënë të qëndrueshme) midis sendit dhe veprimit penal të kundërligjshëm.*

Kolegji Penal verën se, megjithëse kemi të bëjmë me një marrëdhënie midis sendit dhe veprës penale të kryer, jurisprudenca e GjEDNj-së, ***(Vendimi datë 20.01.2009, Sud Fondi s.r.l, etj. kundër Italisë; vendimi datë 30.08.2007, Sud Fondi s.r.l, etj. kundër Italisë; Vendimi datë 01.03.2007, Geerings kundër Vendeve të Ulëta****), ka përcaktuar se gjithsesi nuk mund të mos mbahet në konsideratë edhe verifikimi i veprimit të një personi, si dhe duhet të përjashtuar konfiskimi ndaj subjekteve që gjenden jashtë rrethanave të kryerjes së veprës penale, për të cilët provohet prania e mirëbesimit".*

Vendim Nr. 327, datë 05.12.2012, i Kolegjit Penal të Gjykatës së Lartë: *" .... nëse i pandehuri rezulton se nuk ka kryer veprën penale të "Falsifikimit të dokumenteve", nuk ka se si të deklarohet fajtor për veprën e "****Pastrimit të produkteve të veprës penale****".*

.... teoria e së drejtës penale ka pranuar se për të pasur ekzistencën e

1 *Shih cështjen Nr. 696/05 datë 10 Korrik 2007 Dossa Foundations and Others k.Lihtenshtejnit të GJEDNJ*

*elementeve të veprës së "**Pastrimit të produkteve të veprës penale**", **duhet medoemos që pasuria e krijuar apo vlera monetare që ka shërbyer për krijimin e kësaj pasurie, të jetë rrjedhojë e përfitimeve të ardhura nga aktiviteti kriminal i kryer.** "*

Vendim Nr. 224, datë 09.12.2014, i Kolegjit Penal të Gjykatës së Lartë; *" ...*

Prokurori si subjekti procedural nismëtar ka detyrimin ligjor që, në momentin e paraqitjes së kërkesës për konfiskim (kjo vlen edhe për sekuestrimin), të argumentojë se ekziston dyshimi i arsyeshëm i mbështetur në indicje se pasuria, është e krijuar si rezultat i pjesëmarrjes në organizatat kriminale dhe nuk justifikohen ligjërisht në raport me burimet e ligjshme të të ardhurave dhe kur nuk provohet se pasuria ka prejardhje të ligjshme. Prokurorit, në çdo rast, i del si detyrë që të paraqesë përpara gjykatës indicje të mjaftueshme për të provuar dyshimin se pasuria për të cilën kërkohet masa parandaluese është krijuar nga një aktivitet kriminal nga ato që parashikon shprehimisht ligji.

Prokurori në çdo rast ka për detyrë që të identifikojë pasuritë të cilat pretendohen se janë produkt i veprimtarisë kriminale të parashikuar nga neni 3 i ligjit, me qëllim që interesi publik, i cili determinon në vendosjen e kufizimit të pronës të jetë në proporcion me masën që merret duke u vendosur vetëm mbi ato pasuri të cilat e kanë burimin nga aktiviteti kriminal (Vendimi nr. 4, datë 23.02.2011, pika 22 i Gjykatës Kushtetuese).

Vendim Nr. 226, datë 15.12.2016, i Kolegjit Penal të Gjykatës së Lartë: *" ... Kolegji Penal i Gjykatës së Lartë vëren se: Teoria e së drejtës penale ka pranuar se për të pasur ekzistencën e elementeve të veprës së "Pastrimit të produkteve të veprës penale", duhet medoemos që pasuria e krijuar apo vlera monetare që ka shërbyer për krijimin e kësaj pasurie, të jetë rrjedhojë e përfitimeve të ardhura nga aktiviteti kriminal i kryer. ..."*

Vendim Nr. 5410/201 Akti, datë 24.01.2020, i Gjykatës së Rrethit Gjyqësor Tiranë, marrë formë të prerë i pa-ankimuar**.** Vendim në të cili vetë Prokuroria e Rrethit Gjyqësor Tiranë, ka paraqitur kërkesën e saj me objekt: "***Pushimin e çështjes penale***", pasi në përfundim të gjithë hetimit paraprak të kryer, nuk është arritur të provohej se, prona e pretenduar si "***produkt i veprës penale***", të lidhej apo të buronte nga ekzistenca e një vepre penale "***mëmë***"; ..... ****

Vendim Nr. 9/80, datë 12.03.2021, **i Gjykatës së Posaçme të Shkallës së Parë për Korrupsionin dhe Krimin e Organizuar**, vendim bazuar

në të cilin gjykata e ka pranuar ankimin e bërë nga subjekti të cilit i ishte sekuestruar prona nga OFL, pasi prokurori në seancë nuk ka arritur të provojë dhe të dokumentojë faktin se, personi në fjalë ishte subjekt i posaçëm i këtij ligji, pra nëse ky i fundit ishte autor apo pjesëmarrës në organizata kriminale, grupe të organizuara kriminale, person i dënuar për ato vepra penale të përcaktuara në ligj, nga të cilat krijohen dhe burojnë produktet të cilat pastrohen më pas; e po kështu gjykata në këtë vendim të arsyetuar ka theksuar ndër të tjera se, që prona e sekuestruar është burim i kryerjes apo i pjesëmarrjes në një aktivitet kriminal. ****

Vendim Nr. 106 Akti, datë 29.10.2019, Gjykata e Shkallës së Parë për Krime të Rënda:

".... Gjykata e gjen me vend të sqarojë se, vepra penale e "Pastrimi i produkteve të veprës penale ose veprimtarisë kriminale",e parashikuar nga neni 287 të këtij Kodi, është një vepër e prejardhur, e cila nuk mund të qëndrojë më vete, e pavarur, nëse nuk provohet se, më parë është kryer një vepër penale tjetër ose një veprimtari kriminale e mëparshme, e cila ka nxjerrë të ardhura financiare ose produkte kriminale, produktet e të cilës pastrohen me anë të kësaj vepre penale.

*Që të ekzistojë vepra penale e pastrimit të produkteve të veprës penale ose veprimtarisë kriminale, duhet që më parë të vertetohet ekzistenca e një vepre penale ose veprimtarie kriminale, e cila ka realizuar produkte të veprës penale dhe këto produkte të veprimtarisë kriminale të pastrohen më pas, nga të pandehurit."*****

IX. KONKLUZIONE DHE PËRFUNDIME

Produktet, të ardhurat e veprimtarisë kriminale , përcaktohen nga një hetim objektiv, i plotë, i gjithanshëm, shterrues, i bazuar në prova dhe në fakte konkrete (ose disa indicje të cilat të marra në harmoni të gjitha së bashku njëra me tjetrën krijojnë bindjen e arsyeshme), duke provuar dhe dokumentuar faktin nëse këta persona (të pandehurit) për shkak të të ardhurave të krijuara në mënyrë të paligjshme nga kryerja e një aktiviteti/ veprimtarie kriminale, apo nga kryerja e një vepre penale nga e cila provohet se janë nxjerrë të ardhura financiare, aktualisht janë zotërues të pasurive (të luajtshme dhe të paluajtshme), etj .

Midis produktit të veprës penale (vepra penale mëmë) nga njëra anë dhe veprës penale të pastrimit të këtij produkti (vepra penale bijë), duhet të ekzistojë gjithmonë lidhje shkakësore ekskluzive dhe e domosdoshme

(condicio sine qua non).

Pra, nëse nuk kemi të konsumuar nga ana objektive një vepër penale mëmë, nuk mund të flitet për pastrim të produktit të saj, pasi produkti sipas nenit 287 të Kodit Penal, duhet të rrjedhë si rezultat i një fakti i cili parashikohet nga ligji si vepër penale.

Nga sa u analizua më sipër mund të arrihet në përfundimin se në sistemin ligjor shqiptar, "***pastrimi i produkteve të veprës penale/pastrimi i parave",*** ka ekzistencë të varur juridike, dhe përgjegjësia penale, sikurse edhe masat parandaluese dhe sekuestrimet pasurore të caktuara, kushtëzohen me nevojën e të provuarit se produktet e pastrimit të veprës penale janë të lidhura me faktet juridike të nisjes së një procedimi penal apo dhënies së një vendimi fajësie të formës së prerë, në lidhje me një vepër tjetër penale nga e cila e kanë prejardhjen/ burimin paratë që pastrohen, dhe se produktet/ paratë që pastrohen e kanë prejardhjen nga një veprimtari kriminale.

Për të arritur në konkluzionin se ndodhemi përpara vepërs penale të "***Pastrimit të produkteve të veprës penale apo të veprimtarisë kriminale***, do të duhet (***sikurse argumenton Gjykata e Lartë, Kushtetuese dhe jo vetëm***), që nga ana e organit të akuzës (Prokurorit) të kryhet një hetim i plotë, i gjithanshëm, i hollësishëm, i detajuar, mbështetur edhe në një analizë të detajuar financiare dhe ekonomike, edhe nëpërmjet kryerjes së një hetimi financiar, mbështetur mbi ekspertiza kompetente të fushës përkatëse, me qëllim për të provuar dhe dokumentuar me prova konkrete, faktin se: Pasuria e luajtshme apo e paluajtshme, e evidentuar, është:

a) Produkt i veprës penale, apo i një veprimtarie konkrete kriminale, pra duhet të provojmë ekzistencën e një vepre penale "***mëmë***";

b) Është pasuri e cila bazuar në analizën financiare të kryer nga ekspertë kompetentë të fushës përkatëse, nuk provon të ketë një burim ligjor dhe të justifikuar financiarisht dhe ligjërisht të krijimit të saj;

c) Të jetë pastruar (*qarkulluar, transferuar, etj*) me qëllim konvertimin e saj në para të pastër,

d) Duke ditur burimin e paligjshëm të pasurisë së manaxhuar;

e) Personi nën akuzë penale (neni 287 K.Penal), duhet të jetë Subjekt i kësaj vepre penale[2] (*i dënuar apo i proçeduar për vepra penale të cilat lidhen me krimin e organizuar*).

Për të provuar se ndodhemi përpara veprës penale të "***Pastrimit të***

2 *Shiko Ligjin Nr. 9284, datë 30.09.2004, i ndryshuar,* ***"Për parandalimin dhe goditjen e krimit të organizuar".***

produkteve të veprës penale apo të veprimtarisë kriminale", nevojitet një hetim penal dhe financiar/pasuror i thelluar, duke ndjekur dhe përgjuar pikërisht hapat e ndërmarra nga subjekti kriminal në konsumimin e anës objektive të kësaj vepre penale. Ndaj nevojitet një kualifikim dhe trajnim i azhornuar dhe i vijuar i autoritetit proçedues, të cilët kryejnë hetimin paraprak të këtyre veprave penale, në fushën e krimit ekonomik.

Referencat ligjore dhe doktrinale:

Kodi Penal Shqiptar

Kodi i Proçedurës Penal Shqiptar

Kushtetuta e Shqipërisë

Vendim Nr. 4, datë 23.02.2011, (pika 22), i Gjykatës Kushtetuese

Vendim Nr. 327, datë 05.12.2012, i Kolegjit Penal të Gjykatës së Lartë

Vendim Nr. 224, datë 09.12.2014, i Kolegjit Penal të Gjykatës së Lartë

Vendim i Kolegjit Penal të Gjykatës së Lartë Nr. 201/2015;

Vendim Nr. 226, datë 15.12.2016, i Kolegjit Penal të Gjykatës së Lartë;

Vendim Nr. 5410/201 Akti, datë 24.01.2020, i Gjykatës së Rrethit Gjyqësor Tiranë, marrë formë të prerë i pa-ankimuar.

Vendim Nr. 9/80, datë 12.03.2021, i Gjykatës së Posaçme të Shkallës së Parë për Korrupsionin dhe Krimin e Organizuar.

Vendim Nr. 106 Akti, datë 29.10.2019, Gjykata e Shkallës së Parë për Krime të Rënda:

KEDRNJ Protokolli 1

*Ligji Nr. 10192 datë 03.12.2009 "**Për parandalimin dhe goditjen e krimit të organizuar dhe trafikimit nëpërmjet masave parandaluese kundër pasurisë**"*

*Nenit 1 pika 3 të Direktivës 2015/49 e 20 Majit 2015 "**Mbi parandalimin e përdorimit të sistemit financiar për qëllime të pastrimit të parave dhe financimit të terrorizmit**";*

*Rregullorja 2015/847 "**Mbi informacionin shoqërues të transfertave***

të fondeve*";*

*Ligji nr. 9917, dt.19.05.2008 "**Për parandalimin e pastrimit të parave dhe inancimin e terrorizmit**", i ndryshuar.*

*Ligjit nr. 8269 datë 23.12.1997 '**Për Bankën e Shqipërisë**", i ndryshuar;*

*Rekomandimi Guy Stessens, "**Money Laundering, A neë international laë enforcement model**";*

*Nr. 80 (10) i Komitetit të Ministrave të Këshillit të Evropës i 27 Qershorit 1980 "**Masat kundër transferimit dhe ruajtjes së fondeve me origjinë kriminale**";*

*Deklarata e 12 Dhjetorit 1988 e Komitetit të Bazelit, "**Mbi parandalimin e përdorimit criminal të sistemit bankar për qëllime të pastrimit të parave**";*

*Konventa e Kombeve të Bashkuara kundër Krimit të Organizuar, ratifikuar më ligjin Nr. **8920 datë 11.07.2002**;*

*Komentar "**E drejta Penale**", Dr. Prof Ismet Elezi;*

AKT NORMATIV Nr. 1, datë 31.1.2020 "PËR MASAT PARANDALUESE NË KUADËR TË FORCIMIT TË LUFTËS KUNDËR TERRORIZMIT, KRIMIT TË ORGANIZUAR, KRIMEVE TË RËNDA DHE KONSOLIDIMIT TË RENDIT E SIGURISË PUBLIK"

ONLINE DRUG TRAFFICKING

PROF ASSOC FABIAN ZHILLA

Senior Fellow

Global Initiative against Transnational Crime

Lecturer of Law

Canadian Institute of Technology, Albania

fabian.zhilla@cit.edu.al

Abstract:

Considering the consequences of the COVID19 lock down to society, the online drug trafficking increased rapidly and methods of online supply also sophisticated further in the last five years. Organised crime groups have developed advanced online trafficking pattern of drugs via mobile applications, untraceable online markets and use of cryptocurrencies methods of payment to reach drug consumer door to door. The new patterns of online drug trafficking have also sparked other avenues of money laundering and disguising of tax evasion proceeds of crime. It has also challenged law enforcement agencies in terms of jurisdiction issues, digital evidences and application of special techniques of investigation. On the other hand, international organised crime groups have applied so far, the online drug trafficking to light drugs such as cannabis, hashish and synthetic drugs targeting youths who are tech savvy. The challenge for law enforcement agencies may increase further if this pattern of drug supply will apply to hard drugs. This paper aims to elaborate on the current patterns of online drug trafficking by cyber organised crime and highlight the main features of its typology. The paper seeks to raise awareness of this new trend of

drug trafficking to academic discussion and draw attention to the challenges posed both to law makers on countering this criminal activity.

Key words: Online drug trafficking, dark web, cryptocurrencies, cyber organised crime, law enforcement agencies

Introduction

It is a known maxim that organised crime (here and after "OC") is always a step ahead of law enforcement agencies. In fact, as this paper will show, OC has the ability to adopt and absorb new developing societal trends which will make OC accessible, flexible, and an efficient service provider in criminal markets such as drug trafficking.[1] The OC is increasingly using technology and exploiting every dark spot of the virtual space to trade, negotiate, make profit but also incur harm. This inevitably calls for a paradigm change on the research to OC and criminal markets in the context of cyber space.

The widespread use of technology has not only influenced our modern life but also it has shaped criminal engagement of society to organised forms of criminal activities.[2] On the other hand, the involvement of OC to cyber space has also increased its risk and minimized its role as a free independent space where people could communicate and establish virtual networks to oppose organised crime and government protection hiding their identities and minimising persecution.[3] The virtual world is gradually populated and exploited by criminal organisations and used as another underworld (i.e. deep web) creating criminal markets and criminal services run by OC.[4]

Technology has therefore facilitated the work of OC and sophisticated its patterns. In addition to other benefits, one of the drawbacks of technology is to bring closer OC to society and especially to vulnerable populations such as youths, uneducated individuals, elders, and people with mental health

1 Felia Allum and Francesca Longo ed. (2010). *Defining and Defying Organised Crime: Discourse, Perceptions and Reality.* Routledge, Taylor & Francis Group, London.

2 Stéphane Leman-Langlois ed. (2008). *Technocrime, Technology, Crime and Social Control*. Routledge, Willan, London.

3 Anita Lavorgna (2019). Cyber-organised crime. A case of moral panic? *Trends Organ Crim* 22, 357–374.

4 E. Rutger Leukfeldt, Anita Lavorgna, Edward R. Kleemans (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *Eur J Crim Policy Res* 23, 287–300.

issues.[5] Research on the nexus between technology and OC is emerging and pushing criminological research to another area, the cyber organised crime (here and after "COC" and also raising questions about new definitions of OC and its main activities.[6] Therefore, the object of this paper is to steer the discussion about the new trends of OC in the context of technology and shed lights to a newly popular criminal service such as online drug trafficking. To achieve this objective, the paper will initially in the *first part*, elaborate on the definitions of OC in the context of cyber space. In *the second part,* a review of the most up to date literature on online drug trafficking will be sought to discuss the typology of cyber organised crime generally. In the *third and fourth parts*, the paper will specifically focus on the current trends and developments of online drug trafficking such as platform of trade and methods of payments. The paper will than conclude with the typology of this criminal activity emphasising its sophisticated patterns.

1. Definition of COC

While the focus of this paper is on the online drug trafficking, the definition of OC from the lenses of the cyber space is important as to address research methodologies and revisit theoretical discussions regarding the typology of online drug trafficking or smuggling. It should be noted that today is difficult to distinguish between OC which operate online or offline or in both spaces. Therefore, it will be hard or not scientific to look for a sanitised definition of cyber organised crime (here and after "COC"). In this context current definitions of OC can be assessed to at least conceptualise generally how a COC can be studied. Sometimes the myriad list of the definitions of OC can also be confusing as many of them have been built based on case studies and different contexts or theoretical approaches. However, their perspectives can only be helpful in so far as there is an academic consensus that definitions are there to help and guide the research rather than to constrain the discussion and analysis. The list of definitions of OC is increasingly developed mainly from the criminological perspective.

There are around 200 definitions of OC collected by Klaus von Lampe which tend to conceptualise OC from different cross cutting perspectives, such as ideology (Howard Abadinsky); modus operandi (Jay

5 Alice Hutchings (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, *Law and Social Change*, 62, 1–20.

6 Thomas J. Holt and Adam M. Bossler (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35, 20–40.

S Albanese); criminal intent (Roy Godson); profit making incentive (James O.Finckenauer); networking (Don Liddick)[7]; social approach (Best and Luckenbill); services (Beirne and Messerschmidt); factors (Robert S.Clark); activities (John E. Conklin); perseverance (Donald R.Cressey), behaviour (James O.Finckenauer), illegal markets (Daryl A.Hellman); conspiracy (Wrobleski and Hess); specialisation (Francis A.J. Ianni); transactions (Robert Rhodes); complexity (Patrick J.Ryan); law evading (Schaefer and Lamm); monopolistic approach (Thomas C. Schelling) etc. However, in all this extensive list, very few definitions of OC will include cybercrime as part of the organisational behaviour of criminal groups indirectly and only Tylor Swain (2009) will consider cybercrime in the basket of criminal activities conducted by OC.[8]

1.1. UN Approach

The United Nations Office against on Drugs and Traffic (here and after "UNDOC) however, takes a broader view and as mentioned above tend not only to come out with definition of COC but to broaden the approach which in fact makes it more difficult to grasp with a workable definition of cybercrime. It should be noted that UNDOC has developed the concepts of COC in a teaching platform in 2019, where COC is conceptualised as '*organized criminal groups engaging in cybercrime and cybercriminals or other groups that do not meet the criteria established by the Organized Crime Convention, that engage in activities typically associated with organized crime*'.[9]

According to the UNDOC approach, the COC can also be criminal organisations which do not fall in a proper legal definition of the legislations of UN member countries. In a few words today there is no legal definition of COC in any UN Convention or other international organisations. Coming back to the UN legislation, referring to the UN Convention against Transnational Organised Crime 2000 there are only two definitions which apply to organised forms of crime. First, "Organized criminal group" shall

7 David Bright and Chad Whelan (2021). *Organised Crime and Law Enforcement: A Network Perspective*. Routledge, Taylor & Francis Group, London.

8 See the collection of the definitions of organised crime by Klaus von Lampe available at: http://www.organized-crime.de/organizedcrimedefinitions.htm [accessed on 12 June 2022].

9 See the UNDOC teaching module on cyber organised crime 2019, available at: https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime. [accessed on 12 June 2022].

mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit" (Article 2/a). Second "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure" (Article 2/c). [10] As it seems these definitions need an update to comply to the new trends of OC in the context of cybercrime and online drug trafficking.

Further, the UNDOC, in its teaching module has elaborated on the nexus between OC and technology. Therefore, the OC has used technology to exploit online criminal markets mainly online gambling, to ease their offline activities and as platforms to network with services and other criminal organisations or specialised criminals in the cyber space.[11] As mentioned earlier, UNDOC shows also that considering the flexible nature of OC, today there may be OC focused only on cyber space or criminal organisations which drift between on line and offline criminal world.[12]

1.2. Definition of COC in literature

It should be noted that one of the first comprehensive reports emphasising the new trend of OC in the context of technology was prepared by Michael McGuire in 2012 titled "Organised Crime in the Digital Age". [13] The report notes that OC has entered in the fourth area while the first being the racketeering of the 1920s, the second, the post-World War II black market growth, and the third, the global drug market of the 1970s and 1980s. And the "forth" period is that of digital OC which "combines both on and offline elements, as well as the emergence of disorganized offline groups with a

10 See United Nations Convention against Transnational Organised Crime and the Protocols thereto available at:https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf [accessed on 13 June 2022].

11 See the UNDOC teaching module on cyber organised crime 2019 available at: https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organizedcrime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime. [accessed on 13 June 2022].

12 Peter Grabosky (2007). The Internet, Technology, and Organised Crime. *Asian Journal of Criminology*, 2, 145-161.

13 Michael McGuire (2012). Organised Crime in the Digital Age. *John Grieve Centre for Policing and Security*. London.

common purpose […] using digital tools to enable criminal activity".[14]

This report highlighted some characteristics of COC which is that i) members of this category of OC are young between 25-35 years old ii) around of 50% of analysed groups were composed of 6 or more, with one quarter comprising 11 or more, iii) one quarter of the active groups operated for short periods, less than six months and iii) the purpose of digital tools used for unethical purposes was to enter to offline criminal markets. To this list Broadhurst *et al* (2014) provides an interesting perspective when it comes to the difficulty of defining cyber organised crime.[15] Accordingly, classical features which apply to OC such as number of members, hierarchy, division of roles and conspiracy are minimised by the facilities which are provided by technology. So offline criminal activities would require a number of actors acting in concert together, where in the cyber space these can be conducted by one or two persons with relevant skills.

On the other hand, Broadhurst *et al* (2014) notes also that in contrast with the profit-making motives, violence or corruption which often drive off line OC, in the case of COC can also be conducted for non-profit motives by using nonviolent methods. And this will include "*the quest for intellectual challenge, individual or group notoriety, lust (in the case of organized paedophile activity), ideology, rebellion, and curiosity*".[16] In addition, the presence of membership of the COCmis also different and can include "*a variety of hangers-on, camp followers, and accomplices, some of whom will be well aware of their complicity in criminal enterprise, while others may not*".[17] On the other hand, in a COC group, members may play different roles and have a variety of specialisations. Citing the US Federal Bureau of Investigation's Cyber Division in 2010, Broadhurst *et al* (2014) highlighted at least 10 roles which members of a COC can play (i.e., coders, distributers, technicians, hackers, fraud specialists, hosts, cashers, money mules, tellers, and executives).

In a comprehensive study of UNDOC in 2013[18] on cybercrime three main

14 Tamir Eshel (2012). Organised Crime in Digital Age. Counter Terror & Homeland Security, *Defence Update*, available at: https://defense-update.com/20120328_organized_cyber_crime.html [accessed on 14 June 2022].

15 Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon (2014). Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, International Journal of Cyber Criminology,* 8, 1–20.

16 Ibid, p.3.

17 Ibid.

18 UNDOC (2013), Draft Comprehensive Study on Cyber Crime, February 2013, p.46, available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [accessed on 14 June 2022].

COC groups were defined, i) groups that predominantly operate online and commit cybercrimes; ii) groups which operate both offline and online and engage in crimes and cybercrimes; and iii) groups which use technology to facilitate offline crimes.[19] Forms of COC have been evidenced also in Albania.[20] Considering that drug trafficking can be conducted by OC dealing only with this criminal activity but also by poly criminal groups, all above typologies of COC should be considered as involved in online drug trafficking. The paper therefore in the following section elaborate further on the nexus between COC and online drug trafficking.

2. Platforms of online trade

To have a clear understanding of the typology of online drug trafficking for this section a review of 'The Internet Organised Crime Threat Assessment' reports (here and after "IOCTA") prepared by EUROPOL from 2011 to 2021 is conducted.[21] It should be noted from the outset the data provided in these reports is not specified to online drug trafficking but it is mentioned as one of the online criminal activities conducted by COC. The main portion of drug trafficking is still however committed offline via classical patterns by powerful OC groups (IOCTA 2018, p.47). On the other hand, in context of the EU, consumers of online drug trafficking are coming mainly from Germany, the Netherlands, including here the UK. It is interesting however, to highlight that all these countries are not origin countries of hard drugs and even cannabis. Therefore, the IOCTA reports suggest that the whole sale drugs which are shipped or smuggled to these countries is then traded by local vendors. Therefore, online drug market is '*used for mid- or low-volume market sales or sales directly to consumers. Large-volume sales (wholesale) on Darknet markets are relatively uncommon*' (IOCTA 2018, p.49). IOCTA (2011, p.5) notes that technology is used by OC to facilitate all types of offline criminal activities including drug extraction without providing any detail on how this scheme works. The (2014, p.9) IOCTA highlighted that online drug trafficking will require two main factors, i) anonyms market place and ii) anonymous payment mechanisms.

19 See the UNDOC teaching module on cyber organised crime 2019 available at: https://www.unodc.org/e4j/en/cybercrime/module-13/index.html [accessed on 15 June 2022].

20 Fabian Zhilla and Besfort Lamallari (2015). Organised Crime Threat Assessment in Albania, p.95-104, Open Society Foundation, Albania, available at: https://www.osfa.al/sites/default/files/organized_crime_soros.pdf [accessed on 07 June 2022].

21 See all IOCTA reports available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report [accessed on 10 June 2022].

2.1 Anonyms online drug markets

The main online criminal markets are known as Darknets or Darkweb (use software such as the Onion Router or encryption like PGP).[22] And the online anonymous payment mechanisms are often conducted via virtual currencies.[23] Online drug trafficking can take place either in underground forums or criminal marketplaces. Underground forums are closed communities which trade different criminal products or offer criminal services including drug trafficking. They operate under Darknets. The latter operate within the DeepWeb (i.e., not indexed by search engines) using TOR and I2P technologies (IOCTA 2014, p.8) which are frequently used for online drug supply to end-users. On the other hand, the online market places are specialised criminal markets operating also in Darknets known with different names such as Silk Road, Agora, Outlaw, AlphaBay, Hansa or RAMP, where participants can acquire the type of drug they want and service. These Darknet markets allow software enabling anonymisation (e.g., The Onion Router) or encryption (e.g., PGP). It is estimated that for the period 2011-2013 '*around USD 200 million were spend at the Silk Road on purchase of drugs (i.e., cannabis, prescription drugs, MDMA, LSD, heroin and crystal meth*)'.[24]

In 2017 AlphaBay was considered one of the largest Darknet markets, which is believed to have had around 250 000 separate listings for drugs where 30% of the drugs listings related to Class A drugs (IOCTA 2017, p.50). Until 2018, only three of them, AlphaBay and Hansa and RAMP had accounted for 87% of all Darknet market activity (IOCTA 2018, p.47).

It is interesting to highlight that majority of these online criminal markets can be found not only in English but also in Finnish, French, Italian, Polish and Russian (IOCTA 2014, p.20). Drug has been also traded in open, decentralised cryptocurrency marketplace such as OpenBazaar (IOCTA 2016, p.48).

---

22 Jane Mounteney, Alberto Oteo and Paul Griffiths (2016). The Internet and drug markets: shining a light on these complex and dynamic systems (p.13-19) in *The Internet and Drug Markets*, European Monitoring Centre for Drugs and Drug Addiction (here and after "EMCDA"), available at: https://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf [accessed on 15 June 2022].

23 For a glossary of terms refer to study of EMCDA (2016). *The Internet and Drug Markets*, p. 135, available at: https://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf [accessed on 12 June 2022].

24 Eileen Ormsby (2015). Silk Road: insights from interviews with users and vendors (p.61-69) in *The Internet and Drug Markets*, European Monitoring Centre for Drugs and Drug Addiction (here and after "EMCDA"), available at: https://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf [accessed on 13 June 2022].

While there is considerable effort by law enforcement agencies to take down Darknet markets, criminal organisations and also individual criminals have invested to open new ones. In 2017, several agencies (FBI, DEA, Dutch National Police, Europol etc) had to cooperate in order to take down two largest Darknet Markets AlphaBay and Hansa where the former reached around 200 000 users and 40 000 vendors (IOCTA 2017, p.51).

One of the consequences of closure of the Darknet markets is loss of investments. The funds of the vendors and participants in these closed Darknet markets were stored within the market infrastructure which were latter hacked and stolen by administrators or other professional hackers. The closure of the large Darknet markets triggered also '*the opening of vendor shops run by a single vendor and secondary markets, i.e., non-English language markets catering to a particular nationality or language group*' (IOCTA 2018, p.43). Some examples of local vendors are e Flugsvamp 2.0 and Silkkittie closed down by the Swedish Police in 2020.[25]

In 2015, more than 50% of EU Member States have investigated drug or payment card related activity on the Darknet (IOCTA 2015, p.52). In addition, in 2014, in the operation "Onymous", '*33 high profile marketplaces and forums were taken out of action and 17 individuals were arrested. It is estimated that the seized sites represented approximately 37% of the market share on the Darknet'*. (IOCTA 2015, ibid).

The community of Darknets is sophisticating. They have created specific search engines which avail the navigation in the Darkweb without being traceable. This has facilitated the search for drug, vendors and their ratings in online crime markets. Some of these search engines were known with names such as Recon, Grams, and Kilos (IOCTA 2020, p.56). There is a tendency of law enforcement agencies to spend effort and close down Darknets. However, this has proved to have a counter effect. Criminals are trying to build short lived Darknets which are opened and closed less than a year. This makes difficult for law enforcement agencies to trace them. So, COC will open for some time, close it again and open it with a different name therefore informing their customers in underground forums (IOCTA 2020, p.56).

Recently, there is a tendency for COC to use what is called Bulletproof host (BPH) which have the same role as offshore accounts. The BPH will host scammers, hackers or cyber criminals facilitating illegal market places

25 See the press release of the Swedish Police available at: https://polisen.se/aktuellt/nyheter/2020/februari/charges-brought-in-extensive-darknet-drug-trade-case/ [accessed on 12 June 2022].

including drug trafficking(IOCTA 2020, p.22).

As mentioned in the context of COC and drug trafficking, misuse of technology is considered as online criminal activity in cases where OC hacks systems controlling the movement and location of shipping containers such as the case of a Dutch drug smuggling OC in 2013. The latter infiltrated the port system to manipulate access of the data in order to allow its group to collect the drug from the container before reaching the legitimate haulier (IOCTA 2014, p.23).

Online drug trafficking is also related with other cybercrimes such as the use of compromised card data (i.e., payment fraud) to make purchases of criminal products and services including drugs in the Darknet. According to IOCTA 2017 (p.43) card fraud is committed by individuals and OC. And this criminal activity is conducted by OC it is 'often linked to other crimes such as trafficking in human beings (THB) or drugs, and illegal immigration – crimes where temporary accommodation is required to facilitate the crime'.

Another trend regarding drug trafficking is the increasing the use of crypto phones (i.e., VPNs). Recently, law enforcement agencies in EU have managed to successfully close down two VPNs, the DoubleVPN8 and Safe-Inet.9 (IOCTA 2021, p.18).

3. Anonymous payment mechanisms

As mentioned, Darknets are platforms which hide the traces of the consumers of online criminal services. COC and byers in Dark web are using cryptocurrencies by anonymising the transactions. And this includes blurring the whole chain of the transaction from the drug purchaser to the transfer of the money to the COC. Since 2014 the most popular cryptocurrencies used are Bitcoin, Monero, Ethereum and Zcash. Bitcoin however is traceable and law enforcers can identify the buyer's transactions back to the point when the bitcoins is purchased online, (the block chain method). Block chain allows access everyone via several services which are freely in the web.[26] However, the Darknet markets will anonymise and separate the links between the Bitcoin owner and the transaction, obscuring the identity of its user.

A known site offering this service was Bitcoin Fog known as a bitcoin

26 For an instruction on how to assess the data in block chain see MongoDB "Blockchain Database: A Comprehensive Guide", available at: https://www.mongodb.com/databases/blockchain-database [accessed on 13 June 2022].

mixer. This site was taken down by the US Law Enforcement agencies in 2021. The site was run by two individuals (i.e., Russian and Swedish citizens). According to the press release of US Department of Justice "*over the course of its decade-long operation, Bitcoin Fog moved over 1.2 million bitcoin – valued at approximately $335 million at the time of the transactions. The bulk of this cryptocurrency came from darknet marketplaces and was tied to illegal narcotics, computer fraud and abuse activities, and identity theft*".[27]

Another form of discussing the traces of Bitcoin via crypto mixers is the use of the CoinJoin. The latter combines transactions of several Bitcoin users making difficult to find out who is how in the transaction. A third method of obfuscating Bitcoin transactions was the use of a dedicated wallet that incorporates many different technologies together such as the DarkWallet.[28] The latter is not reached via standard engines in Dark web. However, Samourai Wallet and Electrum on Tails operate on similar principles as DarkWallet, where instructions on their use can also be found online.[29]

Using cryptocurrencies for online drug purchase is only one of the steps of hiding the traces. The COC is increasingly using different layering techniques of payments including third parties to avoid the location of its members and their accounts. Therefore, as explained in the IOCTA 2017 (p.61) COC will use the so-called money mules which either work for COC or are subcontracted to collect the money from the drug purchaser on behalf of the COC. The money muller will then either transfer this money first in its accounts and then transfer it to the accounts of COC or transfer it directly to COC. Sometimes money mules will conduct several services on behalf of COC such as exchanging cryptocurrencies, withdraw the money and hand them over to COC for a fee. Money mules can either be hacked or subcontracted in underground forums. In a large operation led by Europol in November 2016, around 580 money mules were identified across Europe (IOCTA 2017, p.61).

---

27 US Department of Justice, "Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer", 28 April 2021, available at: https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer [accessed on 14 June 2022].

28 For a detailed analysis of use of the methods of obfuscating Bitcoin transactions see Joseph Cox (2016) Staying in the shadows: the use of bitcoin and encryption in cryptomarkets (p.41-47) in *The Internet and Drug Markets*, European Monitoring Centre for Drugs and Drug Addiction, available at: https://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf [accessed on 14 June 2022].

29 See Jake Frankenfield (2021), "Dark Wallet". Investopedia, 24 June 2021, available at: https://www.investopedia.com/terms/d/dark-wallet.asp#:~:text=Dark%20Wallet%20was%20an%20early,Amir%20Taaki%20created%20Dark%20Wallet [accessed on 16 June 2022].

4. Use of mobile phone applications and social media

Another trend of the smuggling the drug is via the use of mobile applications.[30] This method of drug smuggling can be considered as partly online selling as the use of mobile application is part of online communication. The typical form is by creating a mobile application which allows vendors and consumers to contact each other. Then the purchase order is given via this application and then the distribution of the drug is made via classical forms (e.g. person to person, post, curriers etc). According to the study of Moyle *et al.* (2019) the use of mobile application is preferable by both vendors and buyers as '*a convenient, quick option for connecting buyer and seller. They were often viewed as a valuable intermediary option between cryptomarkets and street dealing, providing 'secure' features and the opportunity to preview product without the requirement for technical expertise'*.[31]

In 2019, Interpol issued a Purple Notice following an international investigation run by Israeli Police which led to the arrest of 42 people in four countries (i.e., Germany, Israel. USA and Ukraine) allegedly running a drug distribution network. This criminal organisation was selling drug via the Telegrass mobile application. According to Interpol '*the Telegrass drugs ring was run like a business. Each suspected drug dealer reportedly chooses the pattern of the delivery and payments, with specific units handling illicit activities and specific drugs, with payments made in cash, bitcoin or with drugs, while disguising the source of the money. Methods of delivery included door-to-door delivery, with designated carriers sometimes disguised as Pizza couriers. Minors are also believed to have bought drugs through Telegrass. During raids conducted at the same time as the arrests, the police found money, drugs and technology used by the group to run the drugs ring over the Internet.*'[32]

The purchase of drug is also conducted via main stream social platforms like Tinder and Instagram. This method is mainly used by youths. Borromeo (2016) describes the typology of this drug smuggling by noting that '*buyers can either meet face-to-face or pay online and have their purchases posted*

30 For a list of mobile application see a short article by Annie Lesser (2016) A User's guide to drug apps', Hope&Fears, available at: http://www.hopesandfears.com/hopes/now/drugs/214943-drug-apps [accessed on 10 June 2022].

31 Leah Moyle, Andrew Childs, Ross Coomber, Monica Barratt (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs, *International Journal of Drug Policy*, 63.

32 Interpol 'Online drugs ring: Israel requests INTERPOL Purple Notice', Press Release, 18 March 2019, available at**:** Online drugs ring: Israel requests INTERPOL Purple Notice [accessed on 13 June 2022].

to them. While online payments such as bitcoin and pre-paid gift cards such as Vanilla Visa are encrypted, more traceable measures such as unattributed bank transfers and PayPal are also used. Online dealers mostly sell their drugs as "research" even though pills are put in bottles or blister packs and powders in capsules.'[33]

One of the concerns regarding the use of social media and mobile application is the difficulty of law enforcement agencies to trace the transaction and vendors as social media are platforms accessed by a wide range of users and this makes it hard for the law enforcement agencies to design structured investigation protocol.

5. Conclusion

Online drug trading is getting more sophisticated considering the intricate nature of technology and its constant improvement. As this paper shows, while majority of the drug trafficking is conducted offline, there is a tendency of COC to exploit benefits of virtual space such as anonymity, complicity, easiness, comfort and transborder vulnerabilities to gradually increase the online drug trafficking.

There are three characteristics of the typology of the online drug trafficking. *First*, the modus operandi of COC is mostly based on networking organisational structure from complex to simple ones. *Second*, COC will prefer to trade on untraceable cyber spaces such as Darknets. These markets are short lived and can be divided in two categories, the large once which are open to everyone (i.e., English language markets) and the local markets (i.e., non-English language markets). The use of the Darknets has triggered the creation of specific search engines which are a step further to the sophistication of cybercrime. *Third*, use of encrypted methods of payment conducted via crypto currencies. An important paid in this scheme is played by money mules which can either be hacked or subcontracted by COC in the underground forums. Another popular form of online drug trafficking is the use of mobile application and social media platform.

While the format of this paper was limited to the typology of online drug trafficking it however, highlighted briefly also that this criminal activity is becoming challenging for law enforcement agencies, firstly because of

33 Leah Borromeo 'Drug dealers using Instagram and Tinder to find young customers', The Guardian, 07 April 2016, available at:https://www.theguardian.com/sustainable-business/2016/apr/07/drug-dealers-instagram-tinder-young-customers [accessed on 14 June 2022].

its complex nature and second, that the legal definition of cyber organised forms of criminal activities are not reflected in international legislation. This latter point requires further research and is an avenue to be explored in more depth in term of the consequences to the fight against online drug trafficking.

ZBATIMI I TEKNOLOGJISË SË INFORMACIONIT NË GJYKATA

DR. MAGJISTRAT FATRI ISLAMAJ
Gjykata Apelit Tiranë
fislamaj@beder.edu.al

Abstrakt

Ky punim synon të analizojë lidhjen e Teknologjisë së Informacionit (TI) dhe Inteligjencës Artificiale (IA) me veprimtarinë gjyqësore dhe administrimin e gjykatave. Teknologjia e informacionit mund të aplikohet me një ndikim pozitiv në përmirësimin e performancës në të gjithë sektorët e veprimtarisë së gjykatave, qofshin ato gjyqësore apo veprimtari dhe shërbime administrative. IT dhe IA, rrit performancën e gjykatës në sektorë të ndryshëm, të tilla si administrimi i gjykatës, menaxhimi i rrjedhës së çështjeve, performanca e gjykatës standardet dhe rishikimi periodik i performancës, menaxhimi i burimeve njerëzore, publiku dhe media marrëdhëniet, puna e gjyqtarëve, aksesi në drejtësi, menaxhimi financiar, infrastruktura gjyqësore, mbrojtja dhe siguria në gjykatë, etj.

Zbatimi i suksesshëm i teknologjisë së informacionit në të gjitha këto fusha ndikon drejtpërdrejt në realizimin me sukses të qëllimit dhe misionit të gjykatës, duke siguruar kështu rritjen e besimittë qytetarëve në sistemin gjyqësor.

Fjalët kyçe: Teknologji informacioni, administratë gjyqësore; sistem gjyqësor,siguria kibernetike.

Abstract

This paper aims to analyze the connection of Information Technology (IT) and Artificial Intelligence (AI) with court activities and court administration. Information technology may be applied andhave positive impact on performance improvement in all court activity sectors, ëhether judicialactivity or administrative services. IT and AI, enhances court performance in differet sectors,such as court administration, casefloë management, court performancestandards and periodic performance review, human resources management, public and mediarelations, judges ëork, access in justice, financial management, court infrastructure, protectionand safety in the court,etc.Successful implementation of information technology in all these fields directly impacts thesuccessful realization of the purpose and mission of the court, thus ensuring enhancedcitizen trust in the judicial system.

Keywords: Information technology, court administration; judiciary system, cyber security.

1. Hyrje

Misioni i gjykatave është që ato të zgjidhin me drejtësisi në të gjitha konfliktet gjyqësore që paraqiten para tyre. Ky mision i Gjyqësorit realizohet duke respektuar disa parime themelore siç janë; ai i pavarësisë, paanshmërisë, barazisë paraligjit, të drejtën për një proces të rregullt gjyqësor, përgjegjshmërisë, por dhe llogaridhënies dhe aplikimin parimit "Check and Balances". Aplikimi i teknologjisë së informacionit ne gjykata, lehtëson zbatimin e të gjitha këtyre parimeve që përbëjnë vetë misionin e funksioneve të gjykatave.[1]

Infrastruktura elektronike e teknologjisë së informacionit është konsideruar si një nga elementët kyç të cilët ndikojnë në përmirësimin thelbësor të administrimit efikas të gjykatave[2]. Kjo infrastrukturë elektronike është aplikuar me sukses për të mbështetur veprimtarive që lidhen me

1 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

2 Rekomandimi i Këshillit të Europës 14(2003) i Komitetit të Ministrave të Shteteve Anëtare, datë 09.09.2003 *'The interoperability of information systems in the justice sector'*. Për më shumë shih: https://www.coe.int/t/dghl/cooperation/cepej/series/Etudes7TIC_en.pdf marrë online datë 12.05.2022.

shërbiemet gjyqësore, aksesin në drejtësi, transparencën dhe vlerësimin e performancës së gjykatave.[3]

Teknologjia e informacionit (TI) dhe sistemet ndihmëse të intelegjencës artificiale (IA) po zhvillohen me ritme shumë të shpejta në kohët e sotme. Në këto kushte kjo infrastrukturë teknologjike mund të shërbejë dhe Sistemit Gjyqësor si një mjet që lehtëson zbatimin e parimeve bazë të këtij sistemi. Teknologjia e Informacionit përkufizohet nga Shoqata e Teknologjisë së Informacionit të Amerikës[4] si "*studimi, dizajnimi, zhvillimi, zbatimi, mbështetja ose menaxhimi i sistemeve të informacionit të bazuara në kompjuter, veçanërisht aplikacionet programeve softëer dhe hardueri kompjuterik*"".[5]

Përdorimi efiçent i teknologjisë së informacionit dhe sistemeve të intelegjencës artificiale jep kontribut të rëndësishëm edhe në identifikimin e praktikave më të mira gjyqësore në një kohë më të shpjtë, duke mbështetur edhe në aspekte cilësore përgaditjen e akteve të ndryshme. Studiues të tjerë si Contini and Cordella shprehen se: "*teknologjia e informacionit: ndikon në mënyrën se si ligji interpretohet dhe vihet në zbatim në aspekte të ndryshme si; standartizimi i proceseve dhe procedurave, udhëzon mbledhjen e të dhënava dhe informacionit, përmirëson aksesin ne drejtësi, kontribuan në identifikimin e jurisprudencës dhe prktikave të mëparëshme gjyqësore më të rëndësishme, udhëzon dhe ndihmon nënpunësit gjyqësor dhe magjistratët dhe juristët e tjerë në përgaditjen e akteve apo dokumentave të ndryshëm.*[6]

Në vitet e fundit, shumë vendë europiane kanë aplikuar TI me qëllim që të përmirësojnë efiçencën dhe efikasitetin në gjyqësor [7]. Por gjithsesi, niveli i implementimit të TI varion në mënyrë të ndryshme nga një vend në tjetrin.[8]

---

3 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

4 National Association for Court Management. (2020). Core® Competences. Retrieved from:https://nacmnet.org/who-we-are/initiatives/core-competencies/marrë online datë 18.05.2022.

5 Concetta Manker, 'Factors Contributing to the Limited Use of the Information Technology in State Courtrroms' [2015] Walden Dissertation and Doctorial Studies 1.

6 Contini, F., & Cordella, A. (2015). Assembling law and technology in the public sector: The case of e-justice reforms. Proceedings of the 16th Annual International Conference on Digital Government Research, 124–132. New York, NY. doi:10.1145/2757401.2757418.

7 CEPEJ Guidelines on how to drive change towards Cyberjustice https://www.coe.int/en/ëeb/human-rights-rule-of-laë/-/cepej-publishes-its-guidelines-on-how-to-drive-change-towards-cyberjusticemarrë online datë 14.05.2022.

8 For an overview see European Commission for the Efficiency of Justice, 'European Judicial System' CEPEJ Studies No 24.

Sipas studiuesit Marco Velicogna, këto teknologji mund të ndahen në tre grupe;

Grupi i parë konsiston në teknologjinë bazike si kompjuterat (desktop) dhe sistemet e komunikimit me e-mail, qofshin këto të brendshëm (brenda gjykatës) apo të jashtëm (edhe me subjektet e tjerë)

Grupi i dytë i TI konsiston në aplikacione dhe programe të cilat kryesisht përdoren nga stafi administrative. Ky grup përfshin regjistrat elektronik automatic dhe sistemet e menaxhimit të çështjeve gjyqësore.

Grupi i tretë përfshin teknologjitë që përdoren për të mbështetur punën e gjyqtarëve si baza ligjore elektronik, jurisprudenca gjyqësore më relevante, libraria elektronike, dhe sisteme informative të dënimeve apo sanksioneve.[9] Një Sistem Informativ i Dënimit (SIS) mund të shfaqë gamën e dënimeve për kombinimin e veçantë të veprës penale dhe karakteristikave të shkelësit të zgjedhur, duke bërë të mundur që gjyqtari të shikoje se cili është dënimi i dhënë për një vepër penale nga vendimet e mëparëshme. [10]

Në një Opinion të shpërndarë më dt. 9 Nëntor 2011 Keshilli Konsultativ i Gjyqtarëve Europian (CCJE) theksoi se:"*TI duhet të jetë një vegël apo mjet për të përmirësuar administrimin e drejtësisë, për të lehtësuar aksesin e përdoruesit në gjykata dhe për të përforcuar masat mbrojtëse të përcaktuara në nenin 6 të KEDNJ[11]-së: aksesi në drejtësi, paanshmëria, pavarësia e gjyqtarit, drejtësia dhe kohëzgjatja e arsyeshme e proceseve". dhe vazhdoi duke theksuar se prezantimi i" në gjykatat në Evropë nuk duhet të kompromet*ojë *imazhin dhe humanizmin e drejtësisë.*[12]

Një nga fushat e teknologjisë së informacionit që lidhet drejtëpërdrejtë me kompetencat dhe përgjegjësitë e administrimit të gjykatës, është analizimi i statistikave dhe i treguesve të performancës të gjeneruara nga sistemet elektonike dhe të intelegjencës artificiale të gjykatës përfshirë ato që njihen si Machine learning.[13]

---

9 Marco Velicogna, 'Justice Systems and ICT: What can be learned from Europe' [2007] Utrecht Law Review 129, 130 – 137.

10 Tata C., Wilson J & Hutton N., "*Representations of Knowledge and Discretionary Decision-Making by Decision-Support Systems : the Case of Judicial Sentencing*", Journal of Information Law & Technology-1996 (2).

11 Shih nenin 6 të Konventës Europiane të të Drejtave të Njeriut.

12 Opinion No. (2011)14 of the CCJE, "Justice and information technologies (IT)".

13 Oloruntoba Samson Abiodun dheAkinode John Lekan "*Exploring the potentials of artificial intellgience in the judiciary*" "International Journal of Engineering Applied Sciences and Technology", 2020 Vol. 5, Issue 8, ISSN No. 2455-2143, Pages 23-27 Publikuar Online Dhjetor 2020 in IJEAST (http://www.ijeast.com

Përdorimi i teknologjisë së informacionit në gjykata, kontribuon në konsolidimin garantimit të të drejtave të qytetarëve për akses të barabartë përpara drejtësisë.[14]Në këtë infrastrukturë përfshihen ndër të tjera dhe komjuterat, serverat dhe paisjet elektronike të printimit, sistemet informatikete të informacionit, sistemet elektronike te menaxhimit të çështjeve gjyqësore, sistemet e regjistrimit audio dhe video, sistemet e sigurisë, sistemet e arkivës elektronike dhe gjenerimit të statistikave, sisteme krahasimore dhe evidentimi të ecurise se aspekteve të ndryshme të punës së gjykatave, si dhe faqet e internetit me larmishmëri informacioni për të gjithë subjektet e interesuar për produktin e punës së gjykatës dhe përformancën e saj.[15]

Transparenca është një garanci e cila ndihmon në implementimin e parimeve themelore te punës së gjykatave. Është pikërisht TI, e kombinuar dhe me aplikimin te intelegjencës artificiale, e cila tashmë përbën një mekanizëm të rëndësishëm që po kthehet si infrastrukturë e domosdoshmë për një tërësi subjektesh si, për administratorët e gjykatës, gjyqtarët, administratën dhe përdoruesit e shërbimit gjyqësor.

Një nga aspektet e teknologjisë së informacionit në gjykata është edhe regjistrimi audio i seancave gjyqësore në të gjitha sallat e gjykatave të vendit. Ky sistem ka ndikuar ndjeshëm në rritjen e përgjegjshmërisë dhe transparencës në punën e gjykatave.[16] Në këtë mënyrë, ka dhënë një kontribut të rëndësishëmedhe në në përmirësimin e besimit të publikut tek Gjykata.

Sistemet elektronike të menaxhimit të çështjeve, arkivat elektronike të vendimeve dhe të procesverbaleve të seancave, të integruara në faqe internet te mirëorganizuara, lehtësojne aksesin dhe transparencën e çdo subjekti të interesuar nga çdo pikë e globit në kohë reale në veprimtarinë dhe të dhënat statistikore të gjykatës.

Në kuadër të transparencës, dhe rritjes së aksesit në gjykata, ato duhet te sigurojnë akses on-line (ne kohe reale) ne faqen e internetit te tyre. Këto faqe interneti duhet të pasqyrojnë sa më shumë të dhëna rreth të gjitha veprimtarive gjyqësore, menaxheriale, dhe të performancës së gjykatave. Inkorporimi i një sistemi efikas dhe modern të menaxhimit të çështjeve gjyqësore, në faqen e internetit të gjykatave, do të bëjë të mundur që të aksesohet arkiva

14 Dory Reiling, *Technology for Justice: How Information Technology can Support Judicial Reform* (Leiden University Press 2009) f. 257 – 279.

15 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

16 Albanian Justice Sector Strengthening Project (Just) Year 3 Annual Implementation Report 2013.

historike e vendimeve gjyqësore, procesverbalet e seancave gjyqësore për palët në proçes, kalendari i gjyqeve, analiza statistikore dhe një pafundësi të dhënash të tjera shumëtë rëndësishme për palët dhe qytetarët.[17]

Sigurimi i transparences duhet te bëhet në mënyrë efektive, por pa cënuar garancitë ligjore për mbrojtjen e të dhënave personale. Duke pasur parasysh që infrastruktuara dixhitale e TI lehtëson aksesin e cdo subjekti në sistemet e të dhënave elektronike, legjislacioni ynë ka parashikuar dhe mjetët e mbrojtjes së privatësisë dhe të dhënave personale në këto sisteme. Për këtë qëllim është miratuar Ligji nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale"[18]i ndryshuar, si dhe udhëzimet përkatëse të Komisionerit[19].

Teknologjia e Informacionit mund të aplikohet dhe të ndikojë pozitivisht ne rritjen e performancës tek të gjithe sektorët e veprimtarisë së gjykatave qofshin keto veprimtari gjyqësore apo shërbime administrative si:funksioni i menaxhimit dhe qarkullimit të çështjeve gjyqësore, vlerësimit periodik të performancës së gjykatës, marrëdhëniet me publikun dhe median, etika, menaxhimi financiar,infrastruktura e gjykatave, menaxhimi i burimeve njerëzore, mbrojtja dhe siguria në gjykatëdhe dhe planifikimi strategjik.[20]

Aplikimi i suksesshëm i teknologjisë së informacionit në të gjithë këto fusha të sipër-cituara ndikon drejtëpërdrejtë në realizimin me sukses të qëllimit dhe vetë misionit të Gjykates[21], duke siguruar kështu rritjen besimit te qytetarëve tek sistemi gjyqësor.[22]

Në kushtet aktuale të zhvillimit të teknologjisë së informacionit, një kujdes i veçantë duhet ti kushtohet sistemeve të sigurisë kibernetike, në infrastrukturën elektronike të të dhënave dhe paprekshmërisë së tyre nga faktor të tretë keqdashës, apo me natyrë kriminale. Investime efiçente dhe

17 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

18 Ligji nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale"i ndryshuar me ligjin nr. 48/2012, ndryshuar me ligjin nr.120/2014

19 Komisioneri per tedrejten e InformimitdheMbrojtjen e teDhenavepersonale.

20 National Association for Court Management. (2020). Core® Competences. Retrieved from:https://nacmnet.org/who-we-are/initiatives/core-competencies/marrë online datë 19.05.2022.

21 Wiggins, E. C. (2006). The courtroom of the future is here: Introduction to emerging technologies in the legal system. Law and Policy in International Business, 28(2) 117-127. doi: 10.1111/j.1467-9930.2006.00222.

22 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

serioze duhet të të zhvillohen në sektorin e sigurisë kibernetike, me qëllim që këto sisteme të mos lejojnë ndërhyrje të paautorizuara apo dëmtim të të dhënave që përmbajnë sistemet elektronike.

2. Zbatimii teknologjisë së informacionit në legjislacionin shqiptar për sistemin gjyqësor.

Përsa i përket aplikimit të teknologjisësë informacionit në gjykata, duhet të kemi parasysh që edhe legjislacioni në Shqipëri ka pësuar një evoluim pozitiv, në vitet e fundit. Rëndësia e aplikimit të teknologjisë së informacionit është pasqyruar edhe në Kushtetutën e Republikës së Shqipërisë. Pas ndryshimeve të bërë në Kushtetutë me ligjin nr.76/2016, datë 22.7.2016[23], është bërë një parashikim i posçëm për teknologjinë e informacionit në gjyqësor. Në nenin 147/a të Kushtetutës përcaktohen kompetancat e Këshillit të Lartë Gjyqësor. Sipas pikës "d" të këtij neni përcaktohet se: "*1. Këshilli i Lartë Gjyqësor ushtron funksionet e mëposhtme: ..*

d) drejton dhe kujdeset për mbarëvajtjen e punës në administratën e gjykatave, me përjashtim të mbarëvajtjes së strukturave të teknologjisë së informacionit në gjykata, e cila rregullohet me vendim të Këshillit të Ministrave; ...."[24]

Kjo dispozitë e Kushtetës duket sikur e kufizon Këshillin e Lartë Gjyqësor përsa i përket administrimit të teknologjisë së informacionit në sistemin gjyqësor. Në fakt një interpretim i zgjeruar i kësaj dispozite nuk do të vinte në përputhje me parimin themelor të pavarësisë së gjyqësorit. Kjo për shkak se edhe administrimi i teknologjisë së informacionit në sistemin gjyqësor është pjesë thelbësore e administrimit të gjyqësorit dhe veprimtarive të tij, kompetenca këto, ekskluzive të gjyqësorit.

Kjo paqartësi është zgjidhur me miratimin e ligjit Nr. 115/2016 "Për organet e qeverisjes së Sistemit të Drejtësisë" i ndryshuar. Në nenin 92 te ligjit është përcaktuar se Këshilli i Lartë Gjyqësor është kompetent për të vendosur lidhur me aspektet më të rëndësishme përsa i përket administrimit elektronik të gjykatave.[25]

---

23 Ligji Nr.76/2016, datë 22.7.2016 "Për disa shtesa dhe ndryshime në ligjin nr. 8417, datë 21.10.1998, Kushtetuta e Republikës së Shqipërisë, të ndryshuar".

24 Neni 147/a i Kushtetutës së Republikës së Shqipërisë.

25 Neni 92 te Ligjit Nr. 115/2016 "Për organet e qeverisjes së Sistemit të Drejtësisë" i ndryshuar përcakton se;
"Sipas nenit 92 të ligjit është përcaktuar : "*Sistemi elektronik i teknologjisë së informacionit*
1. Këshilli i Ministrave miraton rregulla për politikat e përgjithshme shtetërore për sistemin e

Gjithashtu Ligji Nr. 98/2016 "Për Organizimin e Pushtetit Gjyqësor në Republikën e Shqipërisë" në mënyrë të përsëritur parashikon aplikimin e teknologjisë së informacionit. Ky ligj në nenin 25 të tij përcaktohen rregullat e ndarjes elektronike të çështjeve gjyqësore.[26]

---

teknologjisë së informacionit për sistemin e drejtësisë, që ndër të tjera parashikojnë:
a) masat mbrojtëse, të cilat sigurojnë vetëm akses të organeve të sistemit të drejtësisë, përveç rasteve kur të dhënat janë me natyrë statistikore ose kur parashikohet ndryshe në ligj;
b) sigurimin e asksesit të plotë të Inspektorit të Lartë të Drejtësisë në të dhënat që përmbajnë të gjithë sistemet e teknologjisë së informacionit në lidhje me Këshillin e Lartë Gjyqësor, gjykatat, Këshillin e Lartë të Prokurorisë dhe zyrat e prokurorisë;
c) garantimin e mbrojtjes së të dhënave personale dhe konfidencialitetin, si dhe mundësinë e çdo personi për të pasur një proces të rregullt gjyqësor ose mundësinë e një autoriteti publik për kryerjen e një hetimi penal;
ç) për organizimin dhe funksionimin e qendrës së teknologjisë së informacionit për sistemin e drejtësisë pranë njërit prej institucioneve të drejtësisë dhe të përcaktojë kompetencat saj.
2. Në përputhje me politikat e përgjithshme në fushën e teknologjisë dhe sigurisë së informacionit, ***Këshilli i Lartë Gjyqësor, në bashkëpunim me qendrën e teknologjisë së informacionit për sistemin e drejtësisë është përgjegjës për****:*
a) zhvillimin ose pjesëmarrjen në zhvillimin e sistemit elektronik të teknologjisë së informacionit për përdorim në gjykata;
b) menaxhimin, koordinimin, monitorimin dhe mbikëqyrjen e përdorimit të teknologjisë së informacionit në gjykata;
c) përcaktimin e sistemit të zbatueshëm të sistemit elektronik të teknologjisë së informacionit të çështjeve dhe kujdeset që sistemi të përdoret në çdo gjykatë;
ç) përcaktimin e rregullave për funksionimin, dhe sigurinë e sistemit elektronik të menaxhimit të çështjeve dhe për mbrojtjen e të dhënave personale të përdorura dhe të ruajtura nga sistemi;
d) mirëmbajtjen e sistemit elektronik të teknologjisë së informacionit të çështjeve, në përputhje me rregullat e parashikuara në shkronjën "b" të këtij neni;
dh) ofrimin e asistencës teknike për gjykatat në përdorimin e sistemit elektronik të menaxhimit të çështjeve;
e) përmirësimin periodik të sistemit, për të siguruar zbatimin e kërkesave funksionale të gjykatave, të vetë Këshillit dhe të organeve të tjera brenda sistemit të drejtësisë, si dhe për të reflektuar ndryshimet në ligjet procedurale;
ë) sigurimin e saktësisë dhe sigurisë së të dhënave dhe mbrojtjen e të dhënave personale;
f) garantimin që sistemi elektronik i teknologjisë së informacionit të të dhënave gjeneron informacione statistikore, të cilat janë të nevojshme për punën e Këshillit të Lartë Gjyqësor dhe të organeve të tjera dhe që përputhen me standardet europiane për treguesit e punës së gjyqësorit, të tilla si norma e evadimit të çështjeve, numri i çështjeve për gjyqtar, kohëzgjatja mesatare e çështjeve dhe kohëzgjatja e çështjeve në proces në raport me kohëzgjatjen mesatare etj.;
g) përcaktimin e rregullave për përdorimin e detyrueshëm të sistemit elektronik të menaxhimit të çështjeve, njësimin e futjes së të dhënave dhe për saktësinë e të dhënave"

26 Neni 25 i Ligji Nr. 98/2016 "Për Organizimin e Pushtetit Gjyqësor në Republikën e Shqipërisë" i ndryshuar :
"1. Ndarja e çështjeve gjyqësore bëhet me short, i cili realizohet në rrugë elektronike, bazuar në parimet e transparencës dhe të objektivitetit.
2. Kancelari i gjykatës mbikëqyr procesin e organizimit dhe të dokumentimit të ndarjes së çështjeve gjyqësore nëpërmjet shortit, si dhe nënshkruan përcjelljen e praktikës së çështjes gjyqësore te gjyqtari i caktuar.
3. Këshilli i Lartë Gjyqësor miraton rregulla më të hollësishme për programin dhe procedurat e ndarjes së çështjeve me short, të cilat në veçanti përcaktojnë:

Në zbatim të parashikimeve të nenit 92 të ligjt Nr. 115/2016 "Për organet e qeverisjes së Sistemit të Drejtësisë", Këshilli i Ministrave ka miratuar Vendimin (VKM) Nr.972, datë 02.12.2020, "*Për organizimin, funksionimin e përcaktimin e kompetencave të Qendrës së Teknologjisë së Informacionit për Sistemin e Drejtësisë*".

Ligji Nr. 115/2016 "Për organet e qeverisjes së Sistemit të Drejtësisë" ligjetë tjera organike për sistemin e drejtësisë, përcaktojnë që një sërë veprimesh gjyqësore apo administrative bëhen falë aplikimit të teknologjisë së informacionit. Ndërkohë që edhe në Kodet e Procedurave civile, dhe penale tashmë janë përfshirë dispozita që parashikojnë mbajtjen e procesverbaleve me sistem elektronik dhe me regjistrim zanor (audio). Gjithashtu, këto kode parashikojnë mundësinë e njoftimeve elektronike të palëve ndërgjyqëse nëpërmjet përdorimit të paisjeve telefonike apo, apo dhe me internet në adresat elektronike.

Ligji Nr.9880, datë 25.02.2008 "*Për nënshkrimin elektronik*" ka parashikuar njohjen dhe përdorimin e nënshkrimeve elektronike në Republikën Shqipërisë.[27]

---

a) programin për organizimin e shortit, me qëllim që të disponojë karaktere dhe parametra të mjaftueshëm, të cilët sigurojnë standardet më të larta të transparencës dhe të kapaciteteve të gjurmimit;
b) mënyrën transparente të dokumentimit të përgatitjes së shortit;
c) afatet e organizimit të shortit dhe mënyrën e njoftimit paraprak të tij;
ç) kriteret për sigurimin e ndarjes së drejtë të çështjeve ndërmjet gjyqtarëve;
d) rastet dhe kriteret e rindarjes së çështjeve me short, kur është e nevojshme për shkaqe të justifikuara;
dh) kritere transparente dhe objektive për procedurën e përjashtimit të gjyqtarëve nga shorti për shkak të ngarkesës ose për shkak të angazhimit të gjyqtarëve në veprimtari të tjera në funksion të gjykatës apo të pushtetit gjyqësor;
e) kritere transparente dhe objektive për ndarjen e çështjeve në rast mosfunksionimi të sistemit elektronik të çështjeve.
4. Inspektori i Lartë i Drejtësisë kryen rregullisht inspektime të ndarjes së çështjeve me short. Ai kontrollon raportet e sistemit elektronik të paktën një herë në vit."
Gjithashtu në nenin 47 të këtij ligji parashikohet si strukturë e gjykatave Shërbimi i teknologjisë së informacionit.
"*Shërbimet e teknologjisë së informacionit sigurojnë:*
a) mirëmbajtjen dhe administrimin e bazës së të dhënave në gjykatë, të mbajtura në formë elektronike nëpërmjet sistemeve kompjuterike, duke respektuar legjislacionin në fuqi për mbrojtjen e të dhënave personale;
b) ruajtjen e rregullt të statistikave të gjykatës".

27 Neni 4 i Ligji Nr.9880, datë 25.02.2008"*Për nënshkrimin elektronik*" përcakton se: "*Veprimet juridike dhe aktet e hartuara nga personat fizikë dhe juridikë, publikë e privatë, mund të bëhen edhe përmes një dokumenti elektronik, të cilit i bashkëlidhet një nënshkrim elektronik i kualifikuar. Dokumenti elektronik, i cili mban emrin e nënshkruesit dhe nënshkrimin e tij të kualifikuar, ka të njëjtën vlefshmëri ligjore dhe fuqi provuese me formën shkresore*

Gjithashtu, për shkak të lehtësirave që ofron, TI është parashikuar si një infrastrukturë e aplikueshme edhe në një tërësi ligjesh të tjera në fuqi, që rregullojnë fusha të rëndësishme të cilat lidhen në mënyrë të drejtëpërdrejtë apo të tërthortë më veprimtarinë e gjykatave. Të tilla janë ligjet që rregullojnë regjistrimin e pasurive të paluajtëshme (ASHK), Qendra Kombëtare e Biznesit, Gjendja Civile, Qendra e Botimeve Zyrtare, Ministria e Drejtësisë, Sistemet funksionale të Policisë së Shtetit edhe shumë institucione të tjera të rëndësishme.

3. Roli i teknologjisë së informacionit në aktivitetin e Menaxhimit të Qarkullimit të Çështjeve.

TI ka një rol thelbësor në realizimin e një menaxhimi efektiv dhe korrekt të qarkullimit të çështjeve gjyqësore. Nëpërmjet pajisijeve moderne të teknologjisë, (si kompjutera, servera, skanera, fotokopje, sisteme komunikimi dhe informacioni etj) bëhët i mundur një përshpejtim substancial i kohës së mbledhjes së të dhënave të të gjitha kategorive. Gjithashtu kjo infrastrukture elektronike, bën të mundur gjenerimin e të dhënave në kohë reale dhe analizimin e tyre.

Nëpërmjet paisjeve te TI, përshpejtohet dhe behët në mënyrë efikase hartimi i akteve te ndryshme ne fushen e njoftimeve apo konfirmimeve që duhet te bëjë gjykatata si dhe pasqyrimi dhe analizimi i statistikave të plota dhe komplekse.[28]

Aplikimi i një sistemi elektronik (informatik) bashkëkohor të menaxhimit të qarkullimit të çështjeve gjyqësore, me funksionalitete të plota, bën të mundur që të gjitha çështjet gjyqësore, sipas kategorive të ndryshme të jenë lehtësisht të menaxhueshme dhe të evidentohet qarkullimi i tyre nga momenti i paraqitjes se tyre në gjykatë e deri në hapin përfundimtar të arkivimit të tyre. Madje edhe pas arkivimit të dosjeve, nëpërmjet një sistemi bashkëkohor të arkivës elektronike lehtësohet gjetja dhe dhënia e informacionit në kohe reale, për dosjet gjyqësore të arkivuara.

Gjithashtu, ndërtimi dhe funksionimi i një sistemi elektronik të menaxhimit të çështjeve funksional dhe bashkëkohor, ndikon drejtëpërdrejtë në rritjen e shpejtësisë së gjykimit të çështjeve në tërësi dhe zbatimit të parimit të gjykimit të çështjeve brenda afateve të arsyeshme, duke mbështetur kështu

28 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

realizimin e një proçesi të rregull ligjor.

Sistemi elektronik i menaxhimit të qarkullimit të çështjeve duhet të jetë në përshtatje të plotë me të gjitha kërkesat e legjislacionit procedurial dhe ligjet e tjera në fuqi. Sistemi duhet të shërbejë si infratrukturë lehtësuese për të gjithë veprimet administrative, apo proçeduriale, që nga regjistrimi i dosjes, shortimi elektronik i çështjeve të katekorive të caktuara brenda seksioneve përkatëse të gjykatës, duke respektuar kërkesat ligjore, shpërndarja tek gjyqtarët përkatës, ecuria e proçesit të gjykimit, deri në dhënien e vendimit përkatës dhe veprimet pas dhënies së vendimit, deri në arkivimin e dosjes gjyqësore. [29] Ky sistem do ishte i më i plotë nëse do të përfshinte dhe qarkullin dhe ecurinë e çështjes në shkallët e tjera të gjyqësorit, për rastet kur është ushtruar ankim apo rekurs. Pra, duhet të jetë një sistem unik i menaxhimit të çështjeve gjyqësore për të gjitha shkallët e gjyqësorit.

Një sistem i kompletuar me bazë të dhënash dhe funksionalitete bashkëkohore, bën të mundur një menaxhim efikas dhe më të shpejtë të qarkullimit të çështjeve gjyqësore, për gjithë hapat e ecurisë së çështjes gjyqësore nga paraqitja dhe regjistrimi deri në arkivim.

Sistemi duhet të mbulojë gjithë aktivitetet që lidhen me veprimtaritë proceduriale për çështjet civile, penale dhe ato administrative, në gjykatat përkatëse. Ky sistem duhet të jetë në lidhje të ngushtë me gjithë nesistemet e tjerë, në kuadrin e një sitemi të integruar të automatizimit. Sistemi për manaxhimin e çështjeve civile dhe penale duhet minimalisht të përfshijë:

- aktivitetet që lidhen me hapjen e çështjeve të reja në gjykatë (civile, penale dhe administrative);
- aktivitetet që lidhen me shpërndarjen e çështjeve tek gjyqtarët;
- aktivitetet që lidhen me gjykimin e çështjeve dhe seansat perkatese;
- një mekanizem paralajmerimi për çështjet gjyqësore të cilat jane në tejkalim të afateve proceduriale të gjykimit, apo që i afrohen këtyre afateve;
- aktivitetet që lidhen me arkivimin e çështjeve kur ato nuk kanë ankim;
- pasqyrimin e ecurise se çështjeve për të cilat paraqitet ankim dhe kundërankim si dhe fatin e çështjeve në gjykimet e shkallëve më të larta.

29 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

Në kuadër të menaxhimit të qarkullimit të çështjeve, sistemet elektronike luajnë një rol të rendësishëm edhe në manaxhimin e dokumentacionit dhe arkivave (Veprimtaria e administrimit të dokumentacionit) Ky nënsitem do duhet të funksionojë si pjesë integrale e nënsistemeve të mësipërm duke dhënë mundësinë e strukturimit, kategorizimit, indeximit dhe rimarrjes të gjithë informacionit që qarkullon në gjykatë.

4. Kontributi i teknologjisë së informacionit në vlerësimin e sandardeve te performancës.

Gjykatat në ditët e sotme konsiderohen si struktura komplekse, të cilat kërkojnë një administrim profesional dhe bashkëkohor. Kështu, teknologjia e informacionit shërben si infrastrukture dhe mjet i rëndësishëm, për të bërë të mundur implementimin e standardeve të performancës, për fusha të ndryshme të veprimatarisë së gjykatës. Gjithashtu, teknologjia e informacionit si fushë, jep një ndihmë thelbësore në matjen e treguesve të performancës së gjyqtarëve, administratës së gjykatës, sektorëve të caktuar, gjykatës si institucion, apo edhe sistemit gjyqësor në tërësi. Ky informacion mund të gjenerohet periodikisht, ose në çdo moment në kohë reale.[30]

Një rol të madhe në përcaktimin e standardeve dhe matjen e treguesve të performancës, jep veçanërisht implementimi i një sistemi të mirë të menaxhimit të çështjeve gjyqësore, i paisur ky me funksionalitete të shumta, në drejtim te matjes se performancës se sistemit, në nivel gjykate, dhe në nivel gjyqtari individual.

TI ndihmon që performanca të vlerësohet, si në në aspektin sasior ashtu edhe në aspektin cilësor. Pra teknologjia e informacioni kontribuon në vlerësimin dhe rritjen e eficencës, zgjidhjen e çështjeve brenda afateve kohore të arsyeshme, por edhe në aspektin kualitativ, që shërbimet gjyqësore të ofrohen në përputhje me parimet themelore dhe me pritshmërite e qytetarëve. Nëpërmjet një sistemi të mirë të menaxhimit të çështjeve gjyqësore, mund të implementohen të gjithë llojet e treguesve, që aplikohen sot në nivel global për matjen e performancës në aspektin sasior, apo cilësor. Për shembull, mund te implementohen mekanizma dhe funksionalitete për zbatimin e të gjitha udhëzimeve të CEPEJ[31] per matjen dhe rritjen e e efiçences ne gjykata.

30 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

31 (The European Commission for the Efficiency of Justice), organ i Këshillit të Europës për monitorimin e efiçencës në sistemin gjyqësor

Nëpërmjet aplikimit intelegjencës artificiale mund të përfshihen programe komplekse informatike në sistemet e gjykatave, të cilët të bëjnë përpunimin dhe analizimin e të gjitha të dhënave të përftuara nga sistemi i menaxhimit të qarkullimit të çështjeve gjyqësore dhe statistikat elektronike të gjykatës. Këto të dhëna mund ti vihen në dispozicion të gjykatës, stafit menaxhues të saj, institucioneve monitoruese të veprimtarisë së gjykatës si KLGJ, ILD, apo studiusve të ndryshëm, me qëllim që të vlerësohen të gjithë treguesit e performancës, në aspektin sasior apo cilësor, qoftë në nivel gjyqtari, sektori, seksioni, në nivel gjykate, apo në nivel të përgjithshëm të sistemit gjyqësor.[32]

Këto statistika mund t'i shërbejnë në mënyrë shumë efikase edhe studiuesve të ndryshëm nëhartimin e studimeve, që vleresojnë nivelin aktual, apo tendencën (vlerësimi krahasimor) e fenomeneve të ndryshme, që lidhen me drejtësine penale, administrative apo atë civile (familjare, pronësore etj), në evidentimin e problematikave të ndryshme të shoqërisë sonë.

Me qëllim matjen e performancës në aspektin cilësor, gjykatat mund të aplikojnë teknologjinë e informacionit duke bërë sondazhe te nivelit të kënaqshmërisë se përdoruesve të shërbimeve gjyqësore (*user satisfaction survey*). Këto sondazhe duhet të shërbejnë jo vetëm si mjete evidentimi të perceptimit, por dhe si udhezues për të orientuar administratorët e gjyakateve që të marrin masa për përmirësimin e performancës së tyre.

Mbledhja dhe analiza e informacionit rreth performancës së gjykates/ gjyqtarit, siguron që menaxherët e gjykatave të kuptojnë se në cilat drejtime, funksione apo sektorë, duhet të ushtrohet me shume vëmendje, përkushtim dhe energji. Në këtë aspekt, aftesitë e administrimit duhet të plotësohen me risitë që ofron teknologjia e informacionit në funksion te një lidershipi me të mirë dhe efiçent. Duke aplikuar zhvillimet më të fundit të intelegjencës artificiale, në funksion të përmirësimit të performancës dhe për qëllime strategjike të rëndësishme menaxherët e gjykatave do të jenë dhe promotore te ndryshimit pozitiv, kurajozë, të përkushtuar, në një administrim me rezultate më të mira.

5. Kontributi i teknologjisë së informacionit në menaxhimin e burimeve njerëzore, etikën dhe integritetin e tyre

Teknologjia e informacionit me funksionalitetet e veta, mund të japë një

32 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

kontribut esencial edhe në veprimtaritë që lidhen me fushën e menaxhimit e burimeve njerëzore të gjykatës dhe sistemit gjyqësor.Teknologjia e informacionit, mund të të mbulojë gjithë aktivitetet që lidhen me regjistrin themeltar të punonjësve të gjykatës dhe dinamikën e plotësimit të dosjeve të tyre personale, me të dhëna të mjaftueshme për vlerësimin e tyre.

Gjithashtu aplikimi i teknologjisë së informacionit do të jetë i lidhur ngushtësisht me aspektet e performancës individuale të secilit punonjës të gjykatës. Këto sisteme informacioni lehtësojnë identifikimin e nevojave për trajnime të ndryshme të burimeve njerëzore, duke rritur kështu kapacitet në kuptimin cilësor dhe integritetin profesional të tyre.

Aplikimi i teknologjisë së informacionit dhe intelegjencës artificiale në sektorë të ndryshëm të veprimtarisë së gjykatave, apo sistemit gjyqësor në tërësi, ndikon në uljen e nevojës për burime njerëzore, pasi një numër shumë të lartë veprimesh (analitike dhe përllogaritje statistikore apo veprime të tejra), do të mund të bëhen nga sistemet informatike, pa pasur nevojën e angazhimit të punonjësve (ose me me ndërhyrjen minimale të burimeve njerëzore). Në këtë mënyrë TI ndikon dhe në reduktimin e kostove ekonomike të sistemit gjyqësor.[33]

Në aspektin e menaxhimit të përditshëm të burimeve njerëzore, sistemet e teknologjisë së informacionit, ndihmojnë menaxherët e gjykatave dhe administratoret e sistemit gjyqesor duke ju siguruar informacion te detajuar dhe të aktualizuar lidhur me:

- organigramën e gjykatës, me rolet dhe pozicionet përkatëse të secilit punonjës;
- të dhënat e nevojëshme te personelit;
- të dhëna mbi edukimin, eksperiencën dhe trajnimet për gjithë personelin;
- pozicionet vakante dhe aplikimet e mundshme për këto pozicione;
- informacione lidhur me performancën e mëpërparëshme ne punë të gjyqtarëve, stafit menaxhues apo administrativ të gjykatës;
- vlerësimet e performancës së gjyqtarëve, stafit administrativ dhe atij mbështetës.

Në funksion të menaxhimit më të mirë dhe cilësor të gjykatave, mund të

33 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

implementohen programe të intelegjencës artificiale, të cilat ndihmojnë në monitorimin e performancës së të gjitha katekorive të burimeve njerëzore, në gjykata. Këto sisteme monitorimi mund ti shërbejnë organeve të menaxhimit të gjykatës, apo të menaxhimit të të gjithë sistemit gjyqësor, për të konstatuar që në fazat fillestre, të shfaqjes së problematikave të ndryshme, dhe të marrin masat përkatëse, për të siguruar që mos të cënohet performanca e shërbimeve gjyqësore. P.sh. mund të identifikohen rastet kur sektorë të caktuar, apo gjykata të caktuara, ndodhen mbingarkohen me punë tej kapacitetit të zakonshëm dhe kërkohet shtimi i organikës me burime njerëzore.[34]

Teknologjia e informacionit, mund të aplikohet edhe në konsolodimin e standarteve më të larta të etikës së gjyqtarëve, stafit drejtues dhe administrativ në gjykata. Në këtë drejtim kemi njëshembull konkret suksesi. Një kontribut pozitiv, në konsolidimin e standarteve etike dhe të integritetit, ka pasur implementimi i sistemeve të regjistrimit audio të seancave gjyqësore.[35] Gjithashtu sistemet e video-vëzhgimit në sallat e gjyqit dhe në ambjentet e gjykatës kanë një rol pozitiv në këtë aspekt.

Kjo infrastrukturë elektronike, përveç se ndikon në nxitjen e përgjegjshmërisë për sjelljen më të mirë etike, ndihmon dhe strukturat e inspektimit, apo vlersimit të performancës etike të gjyqtarëve, apo stafit administrativ të gjykatës, për të marrë vendimet e duhura në këtë fushë.

Stafi menaxhues e i gjykatave, mund te përdorë teknologjinë e informacionit me shumë sukses edhe ne kontrollin dhe vlerësimin e disiplinës në punë, të të gjithe stafit të gjykatës. Mjafton të kujtojmë këtu sistemin eletronik të hyrje-daljeve në institucion, me karta të paisura me mikroçip elektronik.

Teknologjia e informacionit në mënyrëindirekte, ndikon pozitivisht edhe në përmirësimin e etikës të vetë palëve ndërgjyqëse dhe përfaqësuesve të tyre. Duke pasur parasysh se sjellja e tyre është e regjistruar audio dhe video, këto subjekte ushtrojnë funksionet e tyre në performancën e tyre më të mirë të mundshmë. Duke ndikuar kështu dhë si një formë e vazhdueshme edukimi në konsolidimin e përgjegjëshmërisë, në aspektin etik dhe profesional.

Në mënyrë që të këmi një organizim sa më të mirë dhe efikas të punës

34 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

35 Likmeta, E., *Etika profesionale në drejtësinë penale,*shtëpia botuese "asd_studio", Tiranë, 2016, f. 40.

brenda gjykatës, do të duhet që stafi menaxhues, gjyqtarët dhe administrata te kenë mundësi për të komunikuar me njëri tjetrin, në një kohë sa më të shpejtë dhe të dërgojnë të dhëna nga një zyrë në një tjetër në kohë reale.Në këtë aspekt shërben rrjeti i komunikimit te brendshem i njohur si "*Intraneti*".

Një element i rëndësishëm në ndihmë të gjyqtarëve, mund të jetë dhe libraria ligjore, për të cilën do duhej të jepej gjithashtu mundësia e plotësimit dinamik, me informacionet që do vijnë nga qendra e Botimeve Zyrtare, Gjykata e Lartë, Gjykata Kushtetuese si dhe jurisprudenca e Gjykatës Europiane e të Drejtave të Njeriut. Këtu mund të përfshihen dhe sisteme informative të dënimeve apo sanksioneve dhe sisteme te ngjashme.

6. Roli i teknologjisë së informacionit në marrëdhëniet me publikun dhe median

Në fushën e transparencës, e cila sigurohet nga një komunikim efektiv dhe profesional i gjykates me publikun dhe me mediat, teknologjia e informacionit ka bërë një zhvillim pozitiv të jashtëzakonshëm.

Transparenca ndaj qytetarëve dhe medias, është një mekanizëm thelbësor për të garantuar zbatimin e parimeve themelore te misionit të gjykatave. Përmirësimi i standarteve të transparencës është thelbësor edhe në funksion të rrijes së besimit të qytetarëve te sistemi gjyqësor. TI në kohët e sotme, përbën infrastrukturën më rëndësishme dhe efikase për ta siguruar transparencën dhe aksesin, në raport me përdoruesit e gjykatës dhe me publikun.

Nëpërmjet internetit, paisjeve moderne të teknologjisë së informacionit, të instaluara në gjykatë, si dhe ato në posedimin e qytetarëve (smartphone dhe/ose kompjuter), bëhët i mundur një akses i plotë i publikut, në të gjithë veprimtaritë gjyqësore dhe administrative të gjykatës (në të cilat legjislacioni në fuqi i lejon aksesin). Në mënyrë të veçantë, kjo infrastrukturë teknologjise së informacionit është në interes të subjekteve që janë palë në një konflikt gjyqësor, avokatëve të tyre, institucioneve të ndryshme shtetërore, studiuesve të ndryshëm dhe përfaqësuesve të medias (qoftë asaj tradicionale, qoftë medias on-line).

Në këtë aspekt duhet të kemi parasysh që, transparenca e siguruar nga gjykata, duhet të jetë në përputhje edhe me legjislacionin për mbrojtjen e të dhënave pesonale. Në këtë aspekt menaxherët e gjykatave duhet të kujdesen që në faqen e internetit, të vendosin filtrat e nevojshëm të anonimizimit për publikun, por pa kufizuar aksesin dhe transparencën e veprimtarisë së gjykatës, për palët ndërgjyqëse. Arkiva elektronike e gjykatës ka një vlerë të

rëndësishme edhe në aspektet studimore, nga eksperte, akademikë, studiues të ndryshëm, apo në tërësi rrethin e juristëve të cilët mund të studiojnë jurisprudencën e vendimeve gjyqësore për arsye profesionale.[36]

Besimi i publikut është thelbësor për gjykatat që të përmbushin misionin e tyre. Larmishmëria e audiencave, llojit te informacionit dhe metodave të shpërndarjes, kërkon që drejtuesit e gjykatave të jenë të përkushtuar, për të siguruar transparencën dhe llogaridhënien që pritet nga publiku. Aplikimi efikas i teknologjisë së informacionit dhe programeve moderne informatike, do ti ndihmoje menaxherët e gjykatave që të realizojne me sukses të gjitha aspektet e transparencës së gjykatës.Eshtë pikërisht teknologjia e informacionit e cila bën të mundur ndërtimin e faqes së internetit nëpër gjykata, në të cilën qytetarët mund të marrin lehtësisht dhe në distancë, informacionet e nevojëshme në lidhje me gjykatën dhe veprimtaritë e saj. Në këto faqe interneti aksesohet informacion lidhur lidhur me shërbimet e gjykatës, njoftimet dhe shpalljet publike, shortimin elektronik, kalendarin e gjyqeve, monitorimin e ecurisë së proçesit dhe procesverbalet e seancave, të dhëna statistikore, jurisprudenca e gjykatës dhe shumë informacione të tjera, të cilat mund të shtohen sipas kërkesës dhe nevojës së qytetarëve dhe përdoruesve të gjykatës.

Gjithashtu, pajisjet e teknologjisë se informacionit, lehtësojnë dhënien e informacionit edhe në ambjentet e gjykatës, nëpërmjet monitorëve, kompjuterave dhe kioskave elektronike, të dedikuara si pika aksesi për publikun. Në këto pika aksesi, palët ndërgjyqëse dhe publiku mund të marrin të gjithë informacionin e nevojshëm për; çështjet gjyqësore, ecurinë proceduriale të çështjes, kalendarin elektronik të gjyqeve dhe shumë informacione të tjera të vlefshme.[37]

7. Kontributi i teknologjisë së informacionit në menaxhimin financiar dhe infrastrukturën e gjykatave

Teknologjia e informacionit zbatohet edhe në veprimtaritë apo proceset që gjenerojnë të ardhura apo shpenzime, në aspektin financiar. Kështu që

36 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

37 Një shembull suksesi, referuar standardeve më bashkëkohore të kohes, përsa i përket implementimit të i të gjitha këtyre funksionaliteteve, ka qenë Gjykata e Rrethit Gjyqësor Tiranë, në të cilën nga viti 2003 e në vazhdim ka funksionuar shum mirë faqja e internetit, sistemi elektronik e menaxhimit të çështjeve gjyqësore (ARKIT) dhe një sërë pajisesh të tjera të teknologjisë së informacionit. Shih faqen; http://gjykatatirana.gov.al/

kjo infrastrukturë ju vjen në ndihmë zyrave përgjegjëse, apo funksionarëve që lidhen me manazhimin financiar. TI dhe programet e avancuara kompjuterike ndihmojnë specialistës e zyrës së buxhetit në gjykata që të hartojnë, implementojnë dhe ekzekutojnë planet buxhetore, apo të kryjnë operacione dhe analiza të ndrelikuara të kontabilitetit. Teknologjia e e informacionit, i shërben stafit administrues të gjykatës, për të implementuar sisteme intelegjente të menaxhimit të riskut të aseteve financiare, apo te aseteve materiale me vlerë pasurore në gjykata.[38]

Gjithashtu, nëpërmjet rrjeteve të komunikimit elektronik dhe paisjeve të teknologjisë së informacionit, bëhet komunikimi në kohë reale dhe me efikasitet të lartë i gjykatës me institucionet e tjera financiare, (si psh bankat apo dega e thesarit) apo njësinë përkatëse të buxhetit në KLGJ.

Nëpërmjet zbatimit të programeve të intelegjencës artificiale gjykatat, apo dhe vetë sistemi gjyqësor, në nivel qëndror, mund të përfitojnë të dhëna në kohë reale për nevojat buxhetore te sektorëve të caktuar apo gjykatave të caktuara. Në këtë mënyrë, stafi menaxhues mund të ndërhyjë në faza fillestare të paraqitjes së nëvojave, duke siguruar që mos të ulet performanca e shërbimeve gjyqësore, ne funksion të arritjes se misionit dhe qëllimeve të gjykatave.

Investimet e suksesshme nëteknologjine e informacionit ndikojn ndjeshëm dhe në reduktimin e kostove ekonomike të gjykatave per burime njerëzore.

Teknologjia e informacionit, është e integruar në shumë aspekte në infrastrukturën e godinave ku ushtrojnë aktivitetin gjykatat dhe luan një rol të rëndësishëm në këtë aspekt.

Godinat e gjykatave, duhet të jenë të pajisura me të gjitha paisjet teknologjke, të cilat bëjnë të mundur ofrimin e shërbimeve të veprimtarisë gjyqësore.

Teknologjia e informacionit përfshihet në infrastrukturën e gjykatave, që nga krijimi i kushteve bazike të punës, siç janë sistemet e ajrit të kondicionuar, ndriçimi, lëvizshmëria ndër kate, sistemet e sigurise, (videovëzhgimi, metal-detectorët etj..) krijimit të aksesit për qytetarët dhe veçanërisht për personat me aftësi ndryshe, (ashensorë, sisteme komunikimi për të verbrit dhe shurdhmemecët etj.) dhe deri tek instalimet e paisjeve të teknologjisë së

38 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

informacionit, në shërbim të ushtrimit të të gjitha veprimtarive të gjykatës (serverat, kompjuteret, prinetrat, fotokopje, rrjetet e video dhe audio regjistrimit, rjetet e telefonisë, internetit dhe intranetit, videokonferencave etj).

Gjithashtu, sistemet e intelegjencës artificiale mund të zbatohen në gjykata për të ekonomizuar përdorimin e energjisë elektrike apo kostos se nevojshme për ajrin e kondicionuar dhe temperaturën e ambjenteve të gjykatës.

Të gjitha këto aplikime të teknologjisë së informacionit, dhe të tjera që janë në zhvillim e sipër, do të kërkojnë instalimet përkatëse dhe të përshtatëshme brenda godinave të gjykatave dhe do të bëhen pjesë integrale e infrastrukturës së gjykatave ne funksion të realizimit të qëllimit dhe misionit të tyre.

8. Roli i IT-së nëmbrojtjen dhe sigurinënë gjykata

Teknologjia e Informacionit ka një rol të rëndësishëm edhe në aspektin e mbrojtjes dhe garantimit të sigurisë në gjykata. Këtë fakt e konstatojmë që nga rrjetet dhe paisjet moderne teknologjike të monitorimit me kamera deri tek sistemet e mbrojtjes kunder zjarrit, sistemet e alarmit, sistemet e hyrjes se kontrolluar dhe te kufizuar me karta të posacme për stafin e gjykatës.[39]

Gjithashtu një rol të rëndësishëm në rritjen e sigurisë në gjykata luajnë instalimet e paisjeve moderne të kontrollit me metal detektor apo të kontrollit për lëndë eksplozive dhe mjete të tjera të rrezikshme të cilat mund vendosen në pikat e posaçme të hyrjes së publikut dhe të palëve.

Teknologjia e informacionit i shërben gjykatës për të rritur standartet e sigurisë edhe në gjykimet penale qoftë për sigurimin e dëshmitarëve të mbrojtur ashtu edhe në rritjen e sigurisë së të gjithë pjesëmarrësve në proçes.[40] Sallat bashkëkohore të gjykimit duhet të jenë të pajisura, ndër të tjera edhe me sisteme të amplifikimit të zërit (fonisë) për të pandehurit e izoluar me xhamin e sigurisë. Po ashtu paisjet teknologjike bëjnë të mundur dhe garantimin e sigurise së dëshmtarëve apo marrjen e dëshmive nga

39 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

40 Islamaj, F., "Information Technology as an Inseparable Component Supporting all Court Activities: Proposing a Model for Albania", Illyrius: International Scientific Review, Nr. 15, 2020, f. 139-162.

dëshmitarë që ndodhen në distanca shumë të largëta me ambjentin (sallën apo godinën e hgjykatës) ku zhvillohet seanca. Kjo bëhët e mundur me anë të internetit dhe sistemeve të komunikimit me videokonferaenca.

9. Siguria kibernetike

Zhvillimi i vrullshëm i teknologjisë së informacionit dhe aplikimi i saj në një fushë të gjerë të shërbimeve dhe aktiviteteve gjyqësore, duhet të shoqërohet domosdoshmërisht edhe me implementimin e masave mbrojtëse përsa i përket sigurisë kibernetike. Për shak të natyrës dhe vetë misionit që kanë sistemet e teknologjisë së informacionit, janë të aksesueshme nga një numër shumë i lartë përdoruesish. Sistemet e teknologjisë së informacionit, përveç faktit që shërbejnë si infrastrukturë për kryerjen e një numri shumë të madh shërbimesh dhe veprimtarishë në gjykata, ato përmbajnë dhe një larmishmëri të dhënash personale të cilat gëzojnë mbrojtje ligjore. Në këtë mënyrë ato janë të ekspozuara edhe ndaj rrisqeve të ndërhyrjes keqdashëse apo kriminale në sistemet kibernetike. Siguria kibernetike duhet të mbrohet nga kërcënimet që mund të vijnë nga kundërshtarë të motivuar politiksht, kriminel apo organizata të motivuara financiarisht, keqdashës me prirje negative apo nga përdorues të autorizuar të pakujdeshëm.[41]

Administratorët e gjykatave, në mënyrë periodike, duhet të marrin masat për trajnimet e posaçme të të gjitha burimeve njerëzore me standartet me të fundit të sigurisë kibernetike. Kurrikula e trajnimeve në këtë fushë, nuk duhet të mjaftohen vetëm me njohjen e dispozitave të Ligjit 2/2017 “Per sigurinë kibernetike”[42], por duhet të përfshijë aplikimin e standarteve më të mira dhe aktualë në nivel ndërkombëtar përsa i përket mbrojtjes së sigurisë kibernetike.[43]

Për të rritur sigurinë kibernetike kërkohen jo vetem investime të shpejta dhe adekuate, por edhe respektim rigoroz i protokollevetë posaçme të sigurisë kibernetike, të cilat duhet të mirëpërcaktohen me akte nënligjore dhe në rregullore të posaçme nga Këshilli i Lartë Gjyqësor dhe Qendra e Teknologjisë së Informacionit për Sistemin e Drejtësisë, duke implementuar

41 Karen Scarfone, Dan Benigni, Tim Grance Cyber, Security Standards National Institute of Standards and Technology (NIST), Gaithersburg, Maryland (2009) aksesuar ne https://www.nist.gov/publications/cyber-security-standards

42 Ligji 2/2017 “Per sigurinw kibernetike”

43 Shih Direktivën (BE) 2016/1148 të Parlamentit Europian dhe të Këshillit, datë 6 korrik 2016, “Mbi masat për një nivel të përbashkët të lartë të sigurisë së rrjeteve dhe sistemeve të informacionit në Bashkimin Europian”. Numri CELEX: 32016L1148, Fletorja Zyrtare e Bashkimit Europian, Seria L, nr. 194, datë 19.7.2016, faqe 1-30.

standartet me te mira që njihen sot në nivel global.

Përfundime

Teknologjia e informacionit, përbën një infrastrukturë ndihmëse bahkëkohore, e cila kontribuon pozitivisht, në rritjen e performancës tek të gjithe sektorët e veprimtarisë së gjykatave, qofshin këto veprimtari gjyqësore, apo shërbime administrative si: administrimi i gjykatës, funksioni i menaxhimit dhe qarkullimit të çështjeve, vlerësimit periodik i standardeve të performancës së gjykatës, marrëdhëniet me publikun dhe median, menaxhimi financiar,infrastruktura e gjykatave, menaxhimi i burimeve njerëzore dhe etikës, mbrojtja dhe siguria në gjykatë.

Nëse duam të kemi një sistem gjyqësor që performon në përputhje me parimet themelore të pavarësisë paanshmërisë, përgjegjshmërisë, efikasitetit dhe transparencës, atëherë duhet të investojmë dhe në përmirësimin e infrastrukturës së teknologjisë së informacionit në të gjithë sektorët e gjykatave dhe të organeve të administrimit dhe monitorimit të sistemit gjyqësor.

Në kushtet aktuale, të zhvillimit të teknologjisë së informacionit, një kujdes i veçantë duhet ti kushtohet sigurisë kibernetike, për mbrojtjen dhe paprekshmërinë e të dhënave dhe funksionimit të sistemeve elektronike, nga çdo lloj ndërhyrje dashakeqëse, e papërgjegjshme, apo me natyrë kriminale. Investime efiçente dhe serioze, duhet të të zhvillohen në sektorin e sigurisë kibernetike, duke u zbatuar standartet më të mira dhe moderne në këtë fushë.

Infrastruktura moderne e teknologjisë së informacionit, mund të japë një kontribut, të qenësishëm dhe afatgjatë, edhe në funksion të përmirësimit të klimës së besimit të publikut te sistemi i gjyqësor, duke kontribuar kështu në realizimin e Shtetit të së Drejtës në Shqipëri.

"SI KA NDIKUAR TEKNOLOGJIA MODERNE NË KRYERJEN E VEPRAVE PENALE, NËPËRMJET SAJ"

DR. PJERETA AGALLIU
Pedagoge e jashtme pranë Departamentit Penal

Abstrakt

Përparimi i teknologjisë, sikurse janë shprehur ekspertë dhe studiues të së drejtës, ka kontribuar shumë në ndryshimin e natyrës së krimit dhe kontrollit të krimit. Teknologjia dhe krimi janë një fushë më e gjerë se kompjuterët dhe telekomunikacioni edhe pse këto mbeten gjeneruesit më të mëdhenj të krimit kibernetik për shkak të aksesueshmëris së lartë[1]. Ky punim synon të japë një panoramë të përgjithshme të ndikimit të teknologjisë në veprat penale, format në të cilat ai shprehet dhe aktualisht cilat janë format e reja të krimit që praktika ka diktuar nga përdorimi i teknologjisë. Sofistikimin e grupeve kriminale dhe krimit të organizuar përmes përdorimit të teknologjive dhe në çfarë forme shprehen ata sot.

Ndikimi i teknologjisë në kryerjen e veprave penale dhe krimet kibernetike në vetvete kanë sjellë disa sfida të reja për drejtësin penale, referuar shtrirjes ndërkombëtare, shpejtësisë së përhapjes dhe sjelljen e pasojave në një masë më të gjerë se krimet e zakonshm, parë kjo në aspektin e mekanizmave kombëtar dhe ndërkombëtar si një domosdoshmëri për të luftuar apo parandaluar krimin kibernetik. Shqipëria tashmë ka ndërmarrë hapat e saj standartizuese konform me standardet ndërkombëtare, por

1 Deeksha Sharma and Manik Dhingra.*"Technology, crime and its changing patterns"*, Law Audience Journal, December 2018;
Shih për më tepër: https://www.lawaudience.com/technology-crime-and-its-changing-patterns/#google_vignette

mbetet ende në faza embrionale për të qenë e sukseshme e vetme në këtë fushë. Ndaj bashkëpunimi ndërkombëtar, ndaj krimit kibernetik, që në fakt nuk është vetëm një nevojë e vendit tonë, por një thirrje e të gjithë aktorëve ndërkombëtarë, për të luftuar këtë formë të krimit i cili ka për subjekt jo vetëm individë, koorporata, biznese, por edhe qeveri (shtete).

Në përmbyllje të këtij punimi është parë me interest edhe dobia që teknologjia sjell në zbulimin e krimeve. Por, nga ana tjetër, ku dështon shteti në përdorimin e teknologjisë apo ndërveprimi me të, për të siguruar prova për zbulimin e ngjarjes kriminale dhe për të parandaluar apo ndëshkuar autorët e veprës penale, duke cënuar herë pas here edhe të drejtat e njeriut, parë kjo në një vështrim të përmbledhur të praktikës së GjEDNj-së.

Fjalët kyçe: *Teknologji, krimi kibernetik, vepra penale, legjislacion, praktika GjEDNj.*

1. Si ka ndikuar teknologjia në veprat penale dhe krimet kibernetike

Teknologjia, aq sa ka evoluar jetën sociale-kulturore-inovative-ekonomike në të gjitha fushat e saj, po aq ka ndikuar në zhvillimin dhe "përmirësimin" e kryerjes së veprave penale, duke mbuluar gjurmët, në një kohë shumë të të shpejë dhe në forma krejtësisht të reja të krimeve tradicionale si: vjedhja, fyerja, bullizmi, ngacmimi, cënimi i ndershmërisë tregtare, cënimi i tregut të lirë dhe konkurrencës, korrupsionin, cënim i sigurisë publike dhe shtetërore, cënim të pronësisë industriale dhe intelektuale e deri tek format e reja të skallavërimit në epokën e teknologjisë.[2]

Ka shumë lloje të ndryshme të krimit në internet dhe të gjitha rastet duhet të merren shumë seriozisht. Disa shembuj përfshijnë vjedhjen e identitetit, mashtrimin e kartave të kreditit, ngacmimet seksuale dhe ngacmimet kibernetike. Kjo është bota në të cilën jetojmë, duke u bërë një problem i tillë që çdokush mund të bëjë "kërdi" kudo në mbarë globin në çdo kohë të caktuar.[3]

Mediat sociale kanë luajtur një rol masiv për ta bërë edhe më të lehtë për kriminelët të kryejnë sulmet e tyre me qëllim të keq ndaj të tjerëve. Facebook, për shembull, kohët e fundit njoftoi se ata kishin kaluar dy miliardë përdorues aktivë mujorë në platformë. Me shifra të tilla, ai thjesht bëhet

2 Po aty

3 Perkins, S., *"How Technology has Changed Crime"*; shih për më tepër: https://study.com/academy/lesson/how-technology-has-changed-crime.html

një shesh lojërash për të gjithë kriminelët e mundshëm dhe profesionistë në internet.[4] Ashtu si këto teknologji në zhvillim ofrojnë një sërë përfitimesh për përdoruesit, po ashtu ato hapin mundësi të reja për krimin dhe devijimin.[5]

Njerëzit, që vazhdimisht e bëjnë jetën e tyre private publike, kanë një shans shumë më të lartë për t'u shënjestruar, pasi të tjerët e dinë se çfarë kanë bërë në jetën e tyre të përditshme. Gabimi i dytë që bëjnë shumica e njerëzve është duke shkëmbyer shumë informacione me njerëz krejtësisht të panjohur.[6]

Krimi kibernetik konsiston në veprimtari të paligjshme të kryera në kompjuter. Krimet tradicionale mund të kryhen gjatë përdorimit të një kompjuteri, por krimi kibernetik përbëhet nga lloje më specifike krimesh, të tilla si skemat e phishing dhe viruset.[7] Disa prej tyre janë:

Phishing - Phishing është praktika e dërgimit të postave elektronike mashtruese në një përpjekje për të mashtruar marrësin, zakonisht me qëllim të marrjes së parave. Një shembull i zakonshëm i një skeme phishing është kur dikush dërgon një mesazh duke i kërkuar marrësit të arkëtojë një çek për ta. Skema funksionon duke mbledhur informacionin tuaj bankar kur depozitoni çekun dhe duke mbajtur të ardhurat e fondeve që i dërgoni. Ata shpesh do të përdorin gjithashtu informacionin në lidhje me llogarinë tuaj bankare ose nga çeku i anuluar ose çdo çek që ju dërgoni, për të krijuar çeqe të reja me informacionin tuaj në të dhe për të vazhduar skemën e tyre të mashtrimit.

Hakerimi – Hakerimi është i ngjashëm me shkeljen dixhitale. Haker-at depërtojnë në rrjetet online, për të shkarkuar në mënyrë të paligjshme informacione konfidenciale, për të manipuluar funksionet dhe në disa raste për të vjedhur identitete. Kjo shpesh arrihet me sulme të drejtpërdrejta në faqet e internetit, duke mashtruar përdoruesit individual, për të shkarkuar programe me qëllim të keq të maskuar si materiale të tjera ose duke fshehur kodin në e-mail. Shpesh ndodh që qëllimi i haker-imit nuk është marrja e informacionit nga kompjuteri i hakuar, por përdorimi i tij si pjesë e një rrjeti kompjuterësh të përdorur, për të sulmuar objektiva më të vlefshëm, si bankat ose entitetet qeveritare, etj. Një haker mund të përdorë informacionin

4 Po aty

5 Richard K. Moule, "Criminal Use of Technology"; shih për më tepër: https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0211.xml

6 Perkins, S.*"How Technology has Changed Crime"*

7 *"What is Cybercrime? - Definition, History, Types & Laws*"; https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html

e kreditit të një personi për t'u shkaktuar dëm të tjerëve ose për të ofruar një mjet shpërqëndrimi për veprime të tjera që ai ose ajo mund të ndërmarrë. E njëjta gjë mund të realizohet në një faqe interneti. Personi mund të përdorë sulme të shtirura kundër sigurisë së një *website* ose rrjeti kompjuterik të sigurt dhe të përdorë aftësitë e tij/saj reale diku tjetër, ndërkohë që sistemi është i mbingarkuar. Kur personi që kryen krime në internet ose nëpërmjet përdorimit të një kompjuteri është një haker, ai ose ajo zakonisht mbulon gjurmët e tij ose të saj, për të siguruar që autoritetet të mos zbulojnë se kush është me të vërtetë përgjegjës. Disa nga këta persona shkaktojnë dëme edhe më të mëdha duke e bërë të duket se dikush tjetër është shkelës i ligjit. Megjithatë, kur një person akuzohet për krime të tilla, është e rëndësishme që ai ose ajo të ketë përfaqësim ligjor[8].

Përndjekja dhe/ose ngacmimi – Disa kriminelë kompjuterikë përdorin internetin si mbulesë për sjellje të tjera të paligjshme si ndjekja, ngacmimi dhe në raste më të vogla, ngacmimi. Gjithnjë e më shumë, lajmet janë të mbushura me histori të adoleshentëve dhe të tjerëve që kryejnë vetëvrasje pas ngacmimeve kibernetike, duke e bërë këtë një nga format e reja më tinëzare të krimit kompjuterik.

Mashtrimet - Janë praktika mashtruese të kryera nga tekno-kriminelët duke përdorur llogari të postës elektronike. Ju mund të merrni një e-mail që kërkon informacione të llogarisë dhe një depozitë të mirëbesimit të fondeve në këmbim të një pagese përfundimtare shumë më të madhe, ose mund të merrni një e-mail që kërcënon veprime ligjore nëse nuk bëni menjëherë një lloj pagese. Mashtruesit e kompjuterave janë shumë të zgjuar dhe shpesh përdorin frikësimin dhe informacionin personal, për të krijuar besueshmëri.

Frikësimi i mediave sociale **-** Teknokriminalët shpesh synojnë llogaritë personale të mediave sociale. Ata mund të krijojnë një llogari të rreme, për të fituar besimin tuaj, më pas ta përdorin atë llogari, për të bërë kërkesa. Ata mund të përdorin shantazhe, për të marrë atë që duan.

Malware **-** *Malware* është një version i shkurtuar i termave 'software me qëllim të keq'. Është një kategori e gjerë që përfshin softwer të tillë si: viruset, trojanët, spyware, ransomware, adware, worms dhe botnets. Në përgjithësi, malware është krijuar, për të dëmtuar pajisjet ose për të vjedhur të dhëna. Një mënyrë e zakonshme, për të përhapur *malware* është vendosja e tij në një lidhje emaili që duket e besueshme, por lidhja në të vërtetë shkarkon një lloj sulmi malware në sistemin tuaj kompjuterik. Mund të kërkohet pagesa

8 Articles by Lawyers, *"How Computers Are Used to Help Commit Crimes"* https://www.hg.org/legal-articles/how-computers-are-used-to-help-commit-crimes-40716

financiare për të rivendosur sistemin në mënyrë që të mund ta përdorni atë. Mënyra më e mirë për të luftuar malware është parandalimi i infektimit të kompjuterit tuaj.

Përvetësimi **-** Përvetësimi dhe mashtrimi janë lloje të tjera të zakonshme të krimit kompjuterik. Dikush që paraqitet si specialist i investimeve mund t'ju afrohet dhe t'ju premtojë botës për një kontribut financiar relativisht të vogël.

Identifikimi i vjedhjes **-** Vjedhja e identitetit është një problem në rritje dhe mund të kryhet lehtësisht përmes kompjuterit. Identifikoni hajdutët në thelb të mbledhin sa më shumë informacion rreth jush që të munden, më pas përdorni këtë informacion për të marrë karta krediti dhe kredi dhe në thelb supozoni jetën tuaj. Efektet mund të jenë shkatërruese.

Krimet e ATM-ve **-** ATM-të (ose makineritë e automatizuara të arkëtimit), që shpërndajnë para mund të gjenden pothuajse në çdo cep të rrugës këto ditë dhe janë një objektiv i zakonshëm i kriminelëve kibernetikë.

Sulmet e softuerit **-** Në këto lloje sulmesh, kriminelët kibernetikë përdorin pajisje elektronike të jashtme, për të instaluar softuer që do të bëjnë që një makinë ATM të bëjë një nga disa gjëra. Për shembull, kriminelët mund të instalojnë një program që e zbraz makinën nga paratë duke e bërë atë të shpërndajë të gjitha fondet brenda. Ata gjithashtu mund të instalojnë programe që do t'u japin atyre akses në kartat e klientit dhe numrat e identifikimit personal.[9]

Tregtia online e mallrave të paligjshme - Shkeljet e të drejtave të pronësisë intelektuale (IPR) janë të përhapura dhe gjithnjë në rritje, fenomen mbarëbotëror, i përkeqësuar nga tregjet online. Ndikimi i falsifikimit është i lartë në Bashkimin Evropian, me produkte të falsifikuara dhe pirate që arrijnë deri në 5% të importeve. Armët e zjarrit tregtohen gjithnjë e më shumë në platformat online duke përfshirë tregjet e "errëta".[10]

Edhe pse krimet e listuara më sipër janë teknokrime me jakë të bardhë, kompjuterët përdoren për të kryer edhe krime të tjera të rënda. Ato përdoren shpesh për të trafikuar pornografi për fëmijë, për t'u përfshirë në shitjen dhe shpërndarjen e drogave të paligjshme dhe kontrabandës, madje edhe për të kërkuar vrasje.

---

9 Technocrime: Forms & Examples, shih për më tepër https://study.com/academy/lesson/technocrime-forms-examples.html; Updated: 03/15/2022

10 Europol Unclassified – Basic Protection Leve, Crime in the age of technology, The Hague, 12/10/2017; https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

Lista e krimeve që gjenerohen nga përdorimi i teknologjive nuk është asnjëherë shteruese, ndaj sa përmendëm mësipër nuk janë të vetmet forma të teknokrimit. Ka shumë forma të tjera të krimit kompjuterik e teknologjik, por këta janë disa shembuj nga më të zakonshmet.[11]

Studiues të ndryshëm kanë bërë një kategorizim të krimeve nisur nga përdorimi i teknologjive. Ky kategorizim është përcaktuar duke e parë teknologjinë si një mjet ndihmës për realizimin e krimit dhe nga ana tjetër ku vetë teknologjia është objekt përmes të cilit realizohet vepra kriminale. Thënë më thjeshtë në kategorinë e parë pëjnë pjesë ato vepra penale të zakonshme të parashikuara në legjislacionin penal, por që me ndihmën e teknologjisë arrijnë të realizohen në një formë më të sofistikuar dhe në një masë më të gjerë, ndryshe janë emërtuar nga studiues si "Krimi i lehtësuar nga kompjuteri". Krimet e lehtësuara nga kibernetikë janë krime që mund të kryhen në internet ose jashtë linje. Roli luajtur nga interneti është për të rritur shkallën, shtrirjen gjeografike dhe shpejtësinë e këtyre krimeve. Shfrytëzimi seksual i fëmijëve në internet mishëron aspektet më të këqija të krimit të lehtësuar nga kompjuteri. Të abuzimi praktik i të miturve të cënueshëm ndodh shumë në botën reale, por kapet, shpërndahen, inkurajohen dhe madje drejtohen përmes internetit. Interneti ofron shkelësit dhe shkelësit e mundshëm me një mjedis në të cilin ata mund të veprojnë me një nivel i rritur i sigurisë dhe anonimitetit, ku ata mund të hulumtojnë, synojnë dhe kujdesin për të miturit abuzimi.[12]

Kategoria e dytë i përket atyre veprave penale të cilat kanë krijuar forma të reja të veprimtarive kriminale, që realizohen vetëm nëpërmjet përdorimit të tëknologjisë. Krimi i varur nga kiberneti mund të përkufizohet si çdo krim që mund të kryhet vetëm duke përdorur kompjuterë. Krimi kibernetik vazhdon të zgjerohet në shtrirje dhe ndikim. Ekonomitë dhe shoqëritë dixhitale janë një objektiv tërheqës për kriminelët kibernetikë. Inovacioni teknologjik ka perspektiva emocionuese për bizneset dhe qytetarët, por gjithashtu krijon vektorë të rinj sulmi për ata kriminelë që kërkojnë të përfitojnë nga këto zhvillime.[13]

11 Combating Computer Crime; https://www.hg.org/legal-articles/combating-computer-crime-31034

12 Europol Unclassified – Basic Protection Leve, Crime in the age of technology, The Hague, 12/10/2017

13 Po aty

1.1 Teknologjia dhe krimi i organizuar

Krimi i organizuar dhe grupet kriminale në BE ka ndryshuar në mënyrë drastike në vitet e fundit – në pjesa më e madhe për shkak të përparimeve në teknologji. Kriminelët adoptojnë shpejt dhe integrohen me teknologjitë e reja ose ndërtojnë modele krejt të reja biznesi rreth tyre. Përdorimi i teknologjitë e reja nga grupet e krimit të organizuar kanë një ndikim në aktivitetet kriminale në mbarë vendin spektrit të krimit të rëndë dhe të organizuar. Kjo përfshin zhvillimet në internet, të tilla si zgjerimi të tregtisë online dhe disponueshmërisë së gjerë të kanaleve të komunikimit të koduar, si dhe të tjera aspekte të inovacionit teknologjik si teknologjia më e aksesueshme dhe më e lirë e dronëve, dhe teknologjitë e avancuara të printimit.

Krimi i organizuar është një kërcënim kyç për sigurinë e BE-së. Grupet kriminale dhe kriminelët individualë vazhdojnë të gjenerojnë fitime shumë miliarda euro nga aktivitetet e tyre në BE çdo vit. Disa pjesë të grupeve kriminale dhe të krimit të organizuar në BE kanë ndryshuar në mënyrë drastike në vitet e fundit - kryesisht për shkak të përparimeve në teknologji që kanë pasur një ndikim të thellë në shoqërinë dhe ekonominë e gjerë. Ndërsa këto përparime kanë dhënë përfitime të mëdha për shoqërinë në përgjithësi, ato shpesh përdoren, abuzohen ose shfrytëzohen për qëllime kriminale.

Gama dhe shumëllojshmëria e përparimeve teknologjike që mund të shfrytëzohen nga kriminelët është i gjerë.[14][15] Asistimi i kriminelëve është në thelb i pafund, por shembujt kryesorë përfshijnë aksesin në të dhënat e detajuara të hartave, duke përfshirë pamjet satelitore dhe të rrugëve për zbulimin, rrugët dhe oraret e transportit, mësimet, udhëzues dhe receta për drogë ose eksplozivë, dhe këshilla për sigurinë operacionale.

Grupet e organizuara kriminale po kalojnë gradualisht nga aktivitetet kriminale tradicionale në operacione më shpërblyese dhe më pak të rrezikshme në hapësirën kibernetike. Ndërkohë që disa organizata kriminale tradicionale po kërkojnë bashkëpunimin e kriminelëve me aftësitë e nevojshme teknike. Tashmë janë shfaqur lloje më të reja të rrjeteve kriminale që veprojnë vetëm në fushën e krimit elektronik. Struktura e këtyre organizatave kriminale është e ndryshme nga organizatat tradicionale të krimit të organizuar. Aktivitetet kriminale zakonisht kryhen brenda rrjeteve kriminale virtuale me shumë aftësi dhe shumë aspekte të përqendruara në takimet online.

Vetë rrjetet mund të përfshijnë nga dhjetë deri në disa mijëra anëtarë

14 Europol i paklasifikuar – Niveli bazë i mbrojtjes

15 Combating Computer Crime, https://www.hg.org/legal-articles/combating-computer-crime-31034

dhe mund të përfshijnë rrjete të lidhura në strukturën e tyre. Pavarësisht nga numri i anëtarëve dhe filialeve, rrjetet kriminale virtuale zakonisht drejtohen nga një numër i vogël kriminelësh me përvojë në internet, të cilët nuk kryejnë krime vetë, por veprojnë më tepër si sipërmarrës. Disa grupe kriminale "elitare" veprojnë si organizata të mbyllura dhe nuk marrin pjesë në forume në internet, sepse kanë burime të mjaftueshme për të krijuar dhe ruajtur zinxhirët e vlerave, për të gjithë ciklin e krimeve kibernetike, dhe për këtë arsye nuk kanë nevojë të kontraktojnë jashtë ose të angazhohen si të huajt në grupe të tjera[16].

Në mënyrë që forcat e rendit të luftojnë efektivisht krimin e mundësuar nga teknologjia, sigurisht që duhet përqafojnë vetë teknologjinë. Teknologjia mund të jetë gjithashtu një ndihmë e rëndësishme për autoritetet e zbatimit të ligjit në luftën kundër krimit të rëndë dhe të organizuar, shpesh duke përdorur të njëjtën teknologji të abuzuar nga kriminelët. Natyrisht, përdorimi i një teknologjie të tillë nga forcat e zbatimit të ligjit ka implikime të konsiderueshme burimesh, jo vetëm për të fituar akses ose pronësi të teknologjisë në fjalë, por për të siguruar këtë trajnimi adekuat është i disponueshëm, për të përfituar nga teknologjia. Të harmonizuara dhe të koordinuara.[17]

Lufta kundër krimit kibernetik ka qenë gjithmonë një problem kompleks për shkak të numrit të përdoruesve të rrjetit TIK, natyrës transnacionale të internetit dhe arkitekturës së tij të decentralizuar. Kriminelët kibernetikë dhe veçanërisht grupet e organizuara kriminale, kanë qenë dhe ndoshta do të mbeten gjithmonë disa hapa përpara ligjvënësve dhe agjensive të zbatimit të ligjit. Krahas forcimit të kuadrit ligjor aktual, përditësimit të legjislacionit të vjetër, harmonizimit të ligjeve në nivel ndërkombëtar, nevojitet edhe bashkëpunimi ndërsektorial në nivel kombëtar si dhe bashkëpunimi ndërkombëtar në zbulimin, hetimin dhe parandalimin e krimeve elektronike të kryera nga grupeve kriminale të organizuara. Kërkohet zhvillimi i një kuptimi gjithëpërfshirës dhe një qasje largpamëse pasi lufta kundër krimit të organizuar kibernetik duket se ka një objektiv lëvizës.

Vendet përballen me problemin e trajtimit kolektiv të këtij problemi ndërkombëtar. Disa shtete thjesht nuk kanë mjetet e nevojshme për t'iu përgjigjur aktiviteteve të kriminelëve të organizuar kibernetikë, atyre mund t'u mungojnë aftësitë teknike ose të kenë të meta ligjore. Zhvillimi i një

16 Cyber Crime and Organized Crime, https://f3magazine.unicri.it/?p=310

17 Europol Unclassified – Basic Protection Leve, Crime in the age of technology, The Hague, 12/10/2017, Përditësuar: 15.03.2022

kuptimi të përbashkët se asnjë vend nuk mund të jetë i sigurt i vetëm në rrjetin global të TIK-ut është shumë i rëndësishëm.

Me mungesën e një strategjie globale për të luftuar krimin e organizuar kibernetik, problemi ka shumë të ngjarë të thellohet në të ardhmen e parashikueshme. Me zhvillimin e rrjeteve të TIK-ut dhe mundësive që ato ofrojnë, grupet kriminale do të përfitojnë nga e gjithë gama e mjeteve dhe modeleve të disponueshme për sektorët legjitimë të ekonomisë. Disponueshmëria e informacionit do ta bënte atë jo vetëm më të aksesueshëm për grupet e organizuara, por edhe më të lehtë për ta nxitjen dhe automatizimin e aktivitetit të tyre të kryerjes së mashtrimit. Gjithashtu ndoshta do të lidhte më shumë kriminelë oportunistë me rrjetet ekzistuese kriminale.

Krimi kibernetik po transformohet në një industri të paligjshme, ku sindikatat janë shumë të sofistikuara dhe janë shumë të vështira për t'u identifikuar. Disa industri të krimit kibernetik do të drejtoheshin vetëm nga grupe të organizuara kriminale, duke kërkuar vazhdimisht zgjidhjet më të reja teknike dhe për krijimin e tregjeve të reja. Si rezultat, ka të ngjarë që ekosistemi i krimit kibernetik të dominohet së shpejti nga organizatat kriminale, pasi rrjetet e krimit kibernetik që tashmë janë bërë ndërkombëtare do të shumëfishonin mundësitë dhe do të arrinin shkallën globale duke shfrytëzuar dobësinë e kornizave ligjore dhe duke kërkuar strehë të sigurta në vende me më pak aftësi për t'i zbuluar dhe luftuar ato. Kjo do ta bëjë luftën kundër krimit kibernetik një detyrë më të vështirë për agjencitë e zbatimit të ligjit. Për shkak të natyrës pa kufij të internetit, problemi i krimit të organizuar kibernetik ka pasoja vërtet globale kur asnjë vend nuk mund të sigurojë siguri vetëm brenda kufijve të tij. Mënyra e vetme për të adresuar problemin është zhvillimi i përgjigjeve afatgjata që do të përfshinin koordinimin dhe harmonizimin e përpjekjeve në nivel kombëtar dhe ndërkombëtar[18].

2. Kuadri ligjor kombëtar dhe ndërkombëtar dhe strategjia në këtë fushë

2.1 Krimi kibernetik dhe qasja ndërkombëtare

Krimet duke përdorur teknologji inovative të cilësuara dhe si krime të reja, mbeten komplekse dhe jo lehtësisht të zgjidhshme për mekanizmat ligjzbatues. Kjo për faktin se këto lloj krimesh përfshijnë përdorimin e teknologjive të ndërlikuara; ka shumë të dyshuar apo viktima dhe një sasi

18 Cyber Crime and Organized Crime, https://f3magazine.unicri.it/?p=310

të konsiderueshme humbjeje ose dëmtimi; përmban forma të ndryshme të krimit. Këto krime nuk janë të lehta për t'u zbuluar, sepse fillimisht nuk janë përcaktuar si vepra penale dhe kështu në shkallë të parë nuk konsiderohen krim, mund të mos jetë e pamundur, por është e vështirë të merren masa ligjore kundër kategorive të reja të krimit.[19]

Konventa e Budapestit[20] është më shumë se një dokument ligjor; është një kornizë që lejon qindra praktikues nga Palët të ndajnë përvojën dhe të krijojnë marrëdhënie që lehtësojnë bashkëpunimin në raste specifike, duke përfshirë situatat emergjente, përtej dispozitave specifike të parashikuara në këtë Konventë. Çdo vend mund të përdorë Konventën e Budapestit si një udhëzues, listë kontrolli ose ligj model. Për më tepër, bërja palë në këtë traktat sjell avantazhe shtesë.[21]

Konventa mbi krimin kibernetik, e hapur për nënshkrim në Budapest, Hungari, në nëntor 2001, konsiderohet marrëveshja ndërkombëtare më e rëndësishme për krimin kibernetik dhe provat elektronike.

Konventa e Budapestit parashikon (i) kriminalizimin e sjelljeve që variojnë nga aksesi i paligjshëm, të dhënat dhe ndërhyrja e sistemeve ndaj mashtrimeve të lidhura me kompjuterin dhe pornografisë së fëmijëve; (ii) mjetet e ligjit procedural për të hetuarkrimin kibernetik dhe prova të sigurta elektronike në lidhje me çdo krim; dhe (iii) bashkëpunim efikas ndërkombëtar.

Ai pajton vizionin e një interneti të lirë, ku informacioni mund të rrjedhë lirshëm dhe të aksesohet dhe të ndahet, me nevoja për një reagim efektiv të drejtësisë penale në rastet e keqpërdorimeve kriminale. Kufizimet janë të ngushta të përcaktuara; hetohen dhe ndiqen vetëm vepra të veçanta penale dhe të specifikohen të dhënat që nevojiten si provat në procedurat penale specifike sigurohen duke iu nënshtruar mbrojtjeve të të drejtave të njeriut dhe sundimit të ligjit.

Konventa plotësohet nga një Protokoll Shtesë që mbulon kriminalizimin e akteve raciste dhe natyra ksenofobike e kryer përmes sistemeve kompjuterike (CETS 189). Negocimi i një Shtese të dytë Protokolli mbi bashkëpunimin ndërkombëtar të zgjeruar dhe aksesin në prova në re është duke u zhvilluar. Ndërsa ky traktat u negociua nga anëtarët e Këshillit të Evropës si dhe

19 Law Audience Journal, *"Technology, crime and its changing patterns"*, December 2018 https://www.lawaudience.com/technology-crime-and-its-changing-patterns/#google_vignette

20 Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001

21 The Budapest Convention and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention

Kanadaja, Japonia, Afrika e Jugut dhe SHBA është e hapur për anëtarësim nga çdo shtet dhe një numër në rritje i vendeve të Afrikës, të Amerikës. Dhe rajoni Azi/Paqësor po e përdorin këtë mundësi në interes të veprimit efektiv të drejtësisë penale mbi krimin kibernetik.[22]

Është e qartë se çdo zhvillim në përdorimin e teknologjisë nga kriminelët duhet të përputhet dhe kundërshtuar nga një përgjigje e përshtatshme dhe efektive e zbatimit të ligjit. Ka një sfidë të qartë këtu për zbatimin e ligjit që jo vetëm të mbajnë ritmin me zhvillimet e reja teknologjike, por me krime në zhvillim dhe një peizazh kërcënimi që ndryshon vazhdimisht.

Për më tepër, shumë aspekte të krimit kibernetik po zhvillohen me shpejtësi, duke kërkuar specifike njohuritë e ekspertëve dhe përdorimi i teknikave më të fundit hetimore dhe dixhitale të avancuara mjetet kriminalistike. [23]

Krimet kibernetike apo thënë ndryshe përdorimi i teknologjisë në mënyrë të paligjshme për të arritur realizimin e objektivave të paligjshme nuk kryhen vetëm nga individ apo koorporata private, por shpeshherë praktika ka treguar se janë edhe shtetet dhe qeveritë e tyre, të cilat kërkojnë të përftojnë informacione sekrete apo të dhëna për biznese apo organizata të mëdha, për t'i përdorur më pas në dobi të tyre.[24] Teknologjia i fuqizon qeveritë dhe aktorët joshtetërorë që të arrijnë shumë përtej kufijve të tyre kombëtarë. Luftimi i çështjeve transnacionale si sulmet kibernetike, terrorizmi dhe propaganda kërkon zhvillimin e rregullave të reja, për të adresuar pasojat negative të teknologjisë. Sulmet kibernetike të profilit të lartë kanë origjinën nga aktorët shtetërorë, por shpesh kanë shënjestruar korporatat dhe organizatat e tjera joqeveritare. Programi i Politikës së Jashtme dhe Instituti i Hagës për Drejtësi Globale me praninë e një grupi panelistësh të shquar, sollën në vemendje rastin e vitit 2014, kur hakerat e qeverisë së Koresë së Veriut sulmuan Sony Pictures dhe kërcënuan se do të zbulonin e-mail-e dhe filma të papublikuar, ndërsa hakerët e Ushtrisë Çlirimtare Popullore në Kinë vodhën sekretet tregtare nga koorporatat amerikane, për të përfituar[25]. Për të penguar sulmet

22 https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

23 Europol Unclassified – Basic Protection Leve, Crime in the age of technology, The Hague, 12/10/2017, Përditësuar: 15.03.2022

24 How Computers Are Used to Help Commit Crimes https://www.hg.org/legal-articles/how-computers-are-used-to-help-commit-crimes-40716

25 Po aty, 'Këtu i referohemi një shëmbulli ku krimet e përdorimit të kompjuterit dhe internetit u zbuluan dhe u përdorën nga qeveria kineze për çështje militariste dhe teknologjike. Informacioni mblidhet përmes sulmeve në internet, si dhe hakerimit për të marrë të dhëna për bizneset e naftës, si dhe shumë kompani dhe organizata të tjera. Informacioni i marrë nga këto biznese të naftës është përdorur për të sulmuar rrjetet e tyre kompjuterike në vende të ndryshme nga Shtetet e Bashkuara deri në Kazakistan. Informacioni në të dhënat financiare, luftërat e ofertave,

kibernetike të ardhshme, u theksua nevojën për të identifikuar publikisht autorët dhe për të rritur sanksionet derisa sulmet të ndalojnë.[26]

Teknologjitë si interneti, mediat sociale dhe telefonat inteligjentë lejojnë individët dhe grupet të kryejnë krime përtej kufijve ndërkombëtarë. Teknologjia zhvillohet shumë më shpejt se ligjet vendase dhe ndërkombëtare që zbatohen për përdorimin e saj përtej kufijve. Disa vende argumentojnë për kontroll më të madh mbi të dhënat e qytetarëve, me kërkesat e lokalizimit për ruajtjen e të dhënave brenda kufijve kombëtarë. Në vend që të formësojnë teknologjinë në përputhje me ligjin ndërkombëtar bazuar në sovranitetin kombëtar, vendet mund të gjejnë mënyra të reja për zbatimin e ligjeve ekzistuese.

Por, një nga pengesat më të vazhdueshme mbetet: e drejta ndërkombëtare është krijuar që kombet sovrane të punojnë përmes mekanizmave ligjorë për të adresuar ankesat me kombet e tjera sovrane. Disa kompani teknologjike tani janë bërë lojtarë kyç ndërkombëtarë, por si aktorë joshtetërorë që nuk kanë nënshkruar MLAT[27], ato ende qeverisen nga ligjet dhe rregulloret kombëtare. Derisa e drejta ndërkombëtare të arrijë këtë realitet, përgjegjësia ndaj normave ndërkombëtare të të drejtave të njeriut mbetet e pakapshme.[28]

Është konstatuar se shumica e akteve të paligjshme që lidhen me kompjuterin janë jashtë kontrollot të agjencive ligjzbatuese. Ligjet uniform ndërkombëtare mund të ndihmojnë në parandalimin e krimeve transnacionale, në mënyrë që kriminelët të mos jenë në gjendje të cënojnë vendet me kontrollet më të vogla. Prandaj Konventat dhe traktatet nuk janë thjesht parime ndërkombëtare por instrumenta efektiv të unifikimit dhe bashkëveprimit në luftën kundër krimit kibernetik.[29]

2.2 Një qasje e shkurtër e legjislacionit shqiptar dhe prespektiva

Përsa i takon legjislacionit, Shqipëria gjendet mes vendeve që ka aderuar

operacionet në punë dhe dokumentacione të tjera të ngjashme u vodhën."

26 Leksioni i Justice Breyer mbi të Drejtën Ndërkombëtare

27 Përdorimi i ndihmës së ndërsjellë juridike Traktatet (Mutual Legal Assistance Treaties (MLAT) për t'u përmirësuar; Përgjimi i ligjshëm ndërkufitar; Procedurat, 12 September 2012; shih për më tepër https://www.icc-portugal.com/images/publicacoes/documentos_gratuitos/Economia_Digital/ICC_policy_statement_on_Using_Mutual_Legal_Assistance_Treaties_(MLATs)_To_Improve_Cross-Border_Lawful_Intercept_Procedures_(2012).pdf

28 As criminals adapt to new technology, so must international law https://www.brookings.edu/blog/techtank/2017/04/21/as-criminals-adapt-to-new-technology-so-must-international-law/

29 Law Audience Journal, Technology, crime and its changing patterns, December 2018 https://www.lawaudience.com/technology-crime-and-its-changing-patterns/#google_vignette

në Konventën e Budapestit[30] dhe Protokollit të saj shtesë[31] dhe nga ana tjetër ka ndryshuar edhe ligjin e brendshëm penal me miratimin e figurave të reja penale që lidhen kryesisht me krimin kibernetik.

Figurat e veprave penale të miratuara në Kodin Penal janë: 1. Mashtrimi kompjuterik (N.143/b)[32]; 2. Hyrja e paautorizuar kompjuterike (N.192/b)[33]; 3. Përgjimi i paligjshëm i të dhënave kompjuterike (N.293/a)[34]; 4. Ndërhyrja në të dhënat kompjuterike (N.293/b)[35]; 5. Ndërhyrja në sistemet kompjuterike (N.293/c)[36]; 6. Keqpërdorimi i pajisjeve (N.293/ç)[37]; 7. Shitja

30 Ligj Nr. 8888, datë 25.4.2002 Për Ratifikimin e *"Konventës për Krimin në Fushën e Kibernetikës"*

31 Ligj Nr. 9262, datë 29.7. 2004, Për Ratifikimin e "*Protokollit Shtesë Të Konventës Për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të Kryera Nëpërmjet Sistemeve Kompjuterike"*

32 Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda material.

33 Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

34 Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

35 Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet. Kur kjo vepër kryhet në të dhënat kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet. Në rastet kur veprimet e parashikuara në paragrafin e parë janë kryer nga një i mitur, ndaj tij do të zbatohen dispozitat e Kodit të Drejtësisë për të Mitur.

36 Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet. Në rastet kur veprimet e parashikuara në paragrafin e parë janë kryer nga një i mitur, ndaj tij do të zbatohen dispozitat e Kodit të Drejtësisë për të Mitur.

37 Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenet 192/b, 293/a, 293/b e 293/c të këtij Kodi, dënohen me burgim nga

e paautorizuar e kartave SIM (N. 293/d).[38]

Ligjet kryesore që lidhen me sigurinë dhe krimin kibernetik janë: - ligji nr. 7895, datë 27.01.1995, *"Kodi Penal i Republikës së Shqipërisë"*; ligji nr. 2/2017, *"Për sigurinë kibernetike"*; ligji nr. 9918, datë 19.05.2008, *"Për komunikimet elektronike në Republikën e Shqipërisë"*, i ndryshuar; ligji nr. 9887, datë 10.03.2008, *"Për mbrojtjen e të dhënave personale",* i ndryshuar; ligji nr. 8457, datë 11.2.1999, *"Për informacionin e klasifikuar",* i ndryshuar; ligji nr. 9880, datë 25.2.2008, *"Për nënshkrimin elektronik"*, i ndryshuar; ligji nr. 107, datë 15.10.2015, *"Për identifikimin elektronik dhe shërbimet e besuara"*, i ndryshuar.[39]

Në zbatim të ligjit janë ngritur mekanizma si Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), i cili ka përgjegjësinë e mbikëqyrjes së zbatimit të Ligjit Nr.9880/2008 *"Për Nënshkrimin Elektronik"*, Ligjit Nr.107/2015 *"Për Identifikimin Elektronik dhe Shërbimet e Besuara"* si dhe Ligji Nr. 2/2017 *"Për Sigurinë Kibernetike"* dhe të akteve nënligjore të nxjerra në zbatim të tyre. Të cilat ofrojnë garanci të shtuara për mbikëqyrjen dhe përdorimit të teknologjisë dhe formave të saj.

Në kuadër të Njësisë së Krimeve Kibernetike të Policisë së Shtetit në vendin tonë ekziston një laborator qendror i mjekësisë ligjore. Laboratori ka mjete dhe pajisje profesionale duke përfshirë hetimin e telefonave celularë dhe CCTV. Sipas pjesëmarrësve në shqyrtim, shumica e rasteve trajtohen nga laboratori i mjekësisë ligjore nuk kanë lidhje me krimin kibernetik. Laboratori kryesisht shqyrton provat fizike të vepra penale të lidhura me kompjuterin. Laboratori aktualisht ka tetë punonjës me ekspertizë dhe çertifikatat për forenzikën celulare. Pjesëmarrësit ishin të shqetësuar se laboratori i mjekësisë ligjore merret me 1000+ raste në vit bazë, ndërkohë që hetimet mund të jenë të gjata dhe kërkojnë kohë. Gjithashtu, ata janë të ftuar sidëshmitarët të paraqesin provat në gjykatë. Prandaj, ka mungesë të kapacitetit për t'u përgjigjur ndaj nevojave aktuale në adresimin e krimit kibernetik. Kishte një konsensus të përgjithshëm midis palët e interesuara se më shumë burime janë të nevojshme për t'i siguruar edhe Njësisë për Krimet Kibernetike si trajnim i vazhdueshëm për punonjësit.[40]

---

gjashtë muaj deri në pesë vjet.

38 Shkelja e rregullave të caktuara për shpërndarjen, shitjen dhe pajisjen me produkte/karta SIM përbën kundërvajtje penale dhe dënohet me burgim nga tridhjetë ditë deri në gjashtë muaj.

39 Ligjet e listuara në përmbajtjen e Strategjisë Kombëtare për Sigurinë Kibernetike (2020-2025).

40 Report On Cybersecurity Maturity Level in Albania, 2018, fq. 58

Angazhimi i Shqipërisë ndaj sigurisë kibernetike dhe qëndrueshmërisë kibernetike ka përparuar krahasuar me shumë vite më parë. Ndërmarrja e inisiativave që shenjojnë transformime të ndryshme kombëtare dixhitale dhe strategjive për siguri kombëtare. Miratimi i Strategjisë Kombëtare Ndërsektoriale *"Axhenda Dixhitale e Shqipërisë 2015-2020"* nga Ministria e Infrastrukturës dhe Energjisë. Strategjia zëvendësoi Strategjinë Kombëtare Ndërsektoriale për Shoqërinë e Informacionit (2008-2013), një dokument kyç në përcaktimin e Sigurisë kibernetike në një nivel të lartë. Axhenda Dixhitale e Shqipërisë (2015-2020) ndërthurte temën e sigurisë kibernetike në të gjithë strategjinë. Garantimi i niveleve të larta të sigurisë për rrjetet e informacionit ishte një nga elementët thelbësor të strategjisë.[41]

Nga ana tjetër, krahas legjislacionit, praktika e rasteve të ndjekura nga prokuroria, gjykimi deri te marrja e masës nga gjykata për vepra penale në fushën e kibernetikës dhe teknologjisë na njeh me disa statistika. Statistikat në dukje disa shifra, në fakt janë një tregues mjaft i rëndësishëm i jo vetëm efektivitetin e ligjit, forcimin e institucioneve, por edhe problematikat e paparashikuara për të cialt duhet marrë një analizë. Analizë e cila ndihmon më pas në maturimin e institucioneve, përmirësimin e legjislacionit dhe efikacitetin e mekanizmave për parandalimin e krimit kibernetik.

Do të ndalemi vetëm në disa momente krahasimore të viteve të fundit mbi krimet teknologjike dhe krimit kompjuterik, për të parë diferencat mes tyre dhe ndryshueshmëria për një periudhë të shkurtër kohore, përftuar nga raporti i Ministrisë së Brendshme.

Krimi Kompjuterik (N.143/b, 192/b, 293/a/b/c/ç) gjatë periudhës pesëvjeçare mars 2017-2021, ka shënuar vlerën më të lartë. Në mars të vitit 2021 me 37 raste të evidentuara, ndërsa në mars të viteve 2017, 2018, 2019 dhe 2020 krimi kompjuterik ka pasur një trend gjithmon në ulje nga viti në vit, përkatësisht me 21, 15, 11 dhe 6 raste. Në muajin mars 2021 ka pasur një rritje me 23% të rasteve të krimeve kompjuterike në një krahasim brenda një muaji nga shkurti 2021 ku janë evidentuar 30 raste të krimit kompjuterik.[42] Përsa i përket kategorive të krimeve kompjuterike, pjesën më të madhe kryesisht e zënë "Veprat Penale në Fushën e Teknologjisë së Informacionit'. Peshën më të madhe kjo vepër ka patur në Mars 2017 duke zënë 71%, ndërsa peshën më të ulët kjo vepër e ka patur gjatë Mars 2020 duke zënë një peshë prej 50.0%. Ndërsa 'Veprat penale të kryera nëpërmjet sistemit kompjuterik'

41 https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

42 Raporti Statistikor Mujor i Ministrisë së Brendshme mars 2021, Analiza e Krimeve Kompjuterike, fq. 66

kanë pasur një trend të luhatshëm dhe peshën më të ulët e kanë patur gjatë mars 2017 me 29%, ndërsa peshën më të lartë e kanë patur në muajin mars 2020 duke zënë një peshë prej 50.0%.[43]

Ndërsa Raporti i Prokurorit të Përgjithshëm mbi kriminalitetin për vitin 2021, konstaton se numri i procedimeve të dërguara për gjykim në gjykatë është rritur nga 6 procedime për vitin 2020 në 10 procedime për vitin 2021. Rritje e numrit të të pandehurve të dërguar në gjykatë nga 8 në 21 pra 2.6 herë, ndërsa numri i të pandehurve të dënuar për vepra penale kundër krimit kompjuterik nuk ka pësuar ndryshime, mbetet 6.[44]

Mashtrimi kompjuterik (neni 143/b i KP) nga të dhënat statistikore për vitin 2021 është konstatuar rritje e procedimeve të regjistruara për vitin 2021 në krahasim me vitin 2020. Falsifikimi kompjuterik (neni 186/a i KP) është rritur nga 33 në 74. Për veprën penale të ndërhyrjes në të dhënat kompjuterike (neni 293/b i KP) numri i procedimeve për 2021 është rritur krahasuar me një vit më parë nga 51 në 70 procedime.[45]

Format e zakonshme të krimit kibernetik që mbizotërojnë në Shqipëri, përfshijnë mashtrimet që lidhen me Internet banking, të tilla si: phishing dhe spam. Edhe kur individët përgjegjës, për veprimtaritë kriminale kibernetike kundër Republikës së Shqipërisë identifikohen, shpesh është e vështirë për agjencitë e zbatimit të ligjit në Republikën e Shqipërisë dhe organizatat ndërkombëtare, që t'i ndjekin ato kur ato janë në juridiksione të kufizuara. Aktualisht vihet re se mungojnë mjetet e nevojshme, për të marrë dhe krijuar inteligjencë kibernetike, duke përdorur burime njerëzore dhe logjistike të nevojshme, për të ushtruar veprimtarinë ligjzbatuese. Rritja e kapaciteteve për t'u përballur me sfidat kibernetike është thelbësore dhe si pasojë duhet të ndryshohen strukturat, qasja, kapacitetet teknike dhe logjistike etj.[46]

Lidhur me sa më sipër, është i nevojshëm harmonizimi i legjislacionit në fushën e sigurisë kibernetike, me atë të BE-së, duke krijuar mekanizmin e plotë dhe të qartë të kodifikuar, për të adresuar saktë problematikat dhe për t'i zgjidhur ato. Gjithashtu është e nevojshme të realizohet, aty ku është e mundur, qasja, nënshkrimi, ratifikimi dhe zbatimi i instrumenteve ndërkombëtare të sigurisë në internet, duke përfshirë shpërndarjen e burimeve të mjaftueshme, sipas prioriteteve kombëtare, duke marrë në konsideratë

43 Po aty, fq. 67

44 Raport i Prokurorit të përgjithshëm mbi kriminalitetin për vitin 2021, fq.167 https://www.pp.gov.al/rc/doc/Raporti_Vjetor_Kuvendit_per_Kriminalitetin_2021_31_03_22_PP_6411.pdf

45 Po aty, fq.169

46 Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025, Fletorja zyrtare. Nr.7, 2021

zhvillimet teknologjike dhe duke zbatuar parimin e teknologjisë neutral.[47]

3. Dobitë e përdorimit të teknologjisë në hetimin dhe zbulimet e krimeve dhe rastet ku cënohen të drejtat e njeriut

Por, si çdo qasje edhe teknologjia ka anën e saj të medaljes duke luajtur një rol të madh në reformat e ligjit, politikbërjes dhe parandalimit të krimit. Janë përcaktuar dy lloje inovacionesh teknologjike që janë inovacioni i bazuar në informacion dhe inovacioni i bazuar në material. Teknologjitë e reja ndihmojnë shkencëtarët e mjekësisë ligjore të zotërojnë aftësi të ndryshme të përballen me përfshirjen aktive në sistemin e drejtësisë penale. Këtu mund të japim shembujt e njësisë së shkencave fizike që shqyrton parimin e gjeologjisë, fizikës e kimisë, ku përmes teknologjisë dhe pajisjeve të reja ishin shumë të dobishëm në zbulimin dhe identifikimin e provave fizike. Ky shenjohet si një kontribut i madh në fushën e mjekësisë ligjore dhe në hetimin e krimit. Nga ana tjetër kemi njësinë biologjike që është kryesisht përgjegjëse për profilizimin e AND-së, duke u konsideruar si mjeti më i fuqishëm i shkencës së mjekësisë ligjore. Teknologjia në fushën balistike të identifikimit të armëve ekzaminimin e tyre; teknologjitë e analizimit të shkrimit të dorës dhe një nga teknikat e reja është njësia e fotografisë dixhitale dhe ultravjollcë, me rreze X deri tek provat e reja që nuk shihen me sy të lirë. Lista e shërbimeve të teknologjisë nuk është shteruese, ajo është e përfshirë në gjurmimin dhe identifikimin e shumë provave të tjera si gjurmët e gishtërinjëve, analiza e zërit, njësia toksikologjike, njësia poligrafike, hetimi i vendit të krimit etj.

Në këtë mënyrë shtetet gëzojnë një sërë instrumentash teknologjik për të ndihmuar evidentimin e provave dhe përdorimin e tyre në realizimin e një drejtësie sa më efikase. Megjithatë pas çdo të drejte qendron detyrimi i proporcionalitetit, standard i rëndësishëm që duhet të respektohet në çdo fazë të procedimit. Kështu shpesh herë është konstatuar shkelje e të drejtave të privatësisë, kur bëhet fjalë për mbajtjen dhe regjistrimin në një bazë të dhënash të materialit gjenetik të një individi pa patur një shkak të ligjshëm dhe të arsyetuar nga organet shtetërore. Gjykata Evropiane e të Drejtave të Njeriut u shpreh se kishte pasur shkelje të nenit 8 (e drejta për respektimin e jetës private) të Konventës Evropiane për të Drejtat e Njeriut, në çështjen *S. dhe Marper kundër Mbretërisë së Bashkuar*. Kjo çështje kishte të bënte me mbajtjen e pacaktuar në një bazë të dhënash të gjurmëve të gishtërinjve, mostrave të qelizave dhe profileve të ADN-së të aplikantëve pasi procedimi

47 Po aty

penal kundër tyre ishte përfunduar me një pafajësi në një çështje dhe ishte ndërprerë në rastin tjetër.

GjEDNj-ja konsideroi në veçanti se përdorimi i teknikave moderne shkencore në sistemin e drejtësisë penale nuk mund të lejohej me çdo kusht dhe pa balancuar me kujdes përfitimet e mundshme të përdorimit të gjerë të teknikave të tilla kundër interesave të rëndësishme të jetës private. Çdo shtet që pretendon një rol pionier në zhvillimin e teknologjive të reja mbante përgjegjësi të veçantë për "arritjen e ekuilibrit të duhur". Gjykata arriti në përfundimin se natyra e përgjithshme dhe pa dallim e kompetencave të mbajtjes së gjurmëve të gishtave, mostrat celulare dhe profilet e ADN-së të personave të dyshuar, por jo të dënuar për vepra penale, siç zbatohen në këtë rast të veçantë, nuk arritën të arrinin një ekuilibër të drejtë midis interesave konkurruese publike dhe private[48].

Nga ana tjetër shteti duhet të jetë i kujdesshëm në procedimin për një vepër penale duke ruajtur proporcionalitetit midis interesit publik dhe mbrojtjes së të drejtave të njeriut.[49]

Po kështu teknologjitë e gjurmimit, të vendodhjes të cilat përdoren nga organizma shtetërorë duke krijuar dhe një bazë të dhënash, kanë domosddoshmëri përcaktimin ligjor, kushtet dhe kriteret në të cilat mund të kryhet, kohëzgjatjen, publikimin e ligjit si dhe masat, për të mbrojtur individin nga abuzimi në përdorimin e këtyre të dhënave.

Rasti *Shimovolos kundër Rusisë* kishte të bënte me regjistrimin e një aktivisti për të drejtat e njeriut në të ashtuquajturën 'data e të dhënave të mbikqyrjes', e cila mblidhte informacione për lëvizjet e tij, me tren ose ajër, brenda Rusisë dhe arrestimin e tij. Gjykata u shpreh se kishte pasur shkelje të nenit 8 (e drejta për respektimin e jetës private) të Konventës. Ajo vërejti se krijimi dhe mirëmbajtja e bazës së të dhënave dhe procedura për funksionimin e saj udhëhiqej nga një urdhër ministror, i cili kurrë nuk ishte publikuar ose nuk ishte bërë ndryshe i aksesueshëm për publikun. Rrjedhimisht, Gjykata konstatoi se ligji i brendshëm nuk tregoi me qartësi të mjaftueshme fushëveprimin dhe mënyrën e ushtrimit të diskrecionit që u

48 Çështja *S. dhe Marper kundër Mbretërisë së Bashkuar*, 4 dhjetor 2008 (Dhoma e Madhe)

49 Shih çështjen *Gaughran kundër Mbretërisë së Bashkuar*, 13 shkurt 2020, Gjykata vendosi se kishte pasur shkelje të nenit 8 (e drejta për respektimin e jetës private) të Konventës, duke konstatuar se Mbretëria e Bashkuar kishte tejkaluar kufirin e pranueshëm të vlerësimit dhe mbajtja në fjalë përbënte një ndërhyrje joproporcionale me të drejtën e ankuesit për të respekti për jetën private, i cili nuk mund të konsiderohej si i nevojshëm në një shoqëri demokratike. Ky i fundit ishte dënuar një kohë pasi në gjendje të dehur duke drejtuar automjetit në Irlandwn e Veriut, ankimi i tij ishte për mbajtjen e pacaktuar të të dhënave personale (ADN profili, shenjat e gishtërinjve dhe fotografi).

jepet autoriteteve vendase, për të mbledhur dhe ruaj informacionin mbi jetën private të individëve në bazën e të dhënave. Në veçanti, ai nuk parashtroi në një formë të aksesueshme për publikun asnjë tregues të garancive minimale kundër abuzimit. Gjykata gjithashtu u shpreh se kishte pasur shkelje të nenit 5 (e drejta për liri dhe siguri) të Konventës[50].

Ka rezultuar shqetësuese në radhët e bizneseve apo kompanive që në çështjet ku hetohet një partner i tyre dhe në provat e ruajtura në serverat përkatës rezultojnë informacione dhe për ta, ata kanë ngritur shqetësimin se duke mos qenë pjesë e hetimit i është cënuar privatësia e informacionit të kompanisë. Në këtë kontekst tre kompani norvegjeze janë ankuar për një vendim të autoriteteve tatimore që urdhëronte auditorët tatimorë që t'u jepeshin një kopje e të gjitha të dhënave në një server kompjuteri të përdorur së bashku nga të tri kompanitë. Kompanitë ankuese pretenduan në veçanti se masa në fjalë ishte marrë në mënyrë arbitrare. Gjykata u shpreh se nuk kishte pasur shkelje të nenit 8 (e drejta për respektimin e banesës dhe korrespondencës) të Konventës. Ajo u pajtua me argumentin e gjykatave norvegjeze se, për arsye efikasiteti, mundësitë e autoriteteve tatimore për të vepruar nuk duhet të kufizohen nga fakti se një tatimpagues po përdorte një 'arkivë të përzier'edhe nëse ai arkiv përmban të dhëna që u përkasin taksapaguesve të tjerë. Për më tepër, kishte masa mbrojtëse adekuate kundër abuzimit.[51]

Një pjesë e madhe e shqetësimeve mbi veprimet e organeve shtetërore kur sekuestrojnë materiale dhe informacione teknologjike dhe komjuterike duke mos ofruar asnjë mjet garancie për mbrojtjen nga abuzimi me to. Konkretisht në çështjen *Ivashchenko kundër Rusisë*[52] që kishte të bënte me kopjimin e të dhënave nga laptopi i një fotoreporteri nga doganierët rusë. Gjykata gjeti shkelje të nenit 8 (e drejta për respektimin e jetës private) të Konventës, duke konstatuar se, në përgjithësi, qeveria ruse nuk kishte treguar se legjislacioni dhe praktika e aplikuar në këtë çështje kishin ofruar garancitë e nevojshme kundër abuzimi kur bëhej fjalë për aplikimin e procedurës së marrjes së mostrave doganore për të dhënat elektronike që përmban një pajisje elektronike.

50 Çështja *Shimovolos kundër Rusisë*, 21 qershor 2011

51 Çështja *Bernh Larsen Holding As dhe të tjerët kundër Norvegjisë*

52 Çështja *Ivashchenko kundër Rusisë*, 14 mars 2013

Konkluzione dhe rekomandime

- Asgjë nuk është plotësisht e sigurtë në botën kibernetike. Krimi kibernetik është bërë një çështje shqetësuese për çdo komb në vitet e fundit.
- Këto krime variojnë nga vjedhja e informacionit nga kompjuteri i një personi në shtëpinë e tij ose të saj deri te sekretet e korporatave të përdorura si avantazh konkurues dhe deri te mashtrimi dhe spiunazhi. Krimet dixhitale janë të gjera dhe ndonjëherë të vështira për t'u ndjekur penalisht me sukses. Pa ligjet e duhura në fuqi, këto shkelje mund të vazhdojnë për dekada me pak ose aspak pasoja.[53]
- Hapi i parë për të mbrojtur veten kundër krimit kompjuterik (ndonjëherë i quajtur edhe 'krim kibernetik') është të kuptosh se çfarë është, për të siguruar një vetëmbrojtje.[54]
- Vetë pajisjet teknologjike kanë shtuar elementë që i mbron ato nga përdorimi i paautorizuar, keqpërdorimi apo përdorimi i mirëfilltë për vepra kriminale, duke u bërë një instrument në gjurmimin e krimit dhe parandalimin e pasojave më të rënda.
- Zhvillimi i një grupi koherent kërkimi mbi përdorimin kriminal të teknologjisë përfshin disiplina dhe teori të sjelljes individuale dhe grupore. Në të vërtetë, vlen të përmendet se këto fusha janë shqetësime jo vetëm për kriminologjinë, por edhe për shëndetin publik, zhvillimin njerëzor, shkencat kompjuterike, ekonominë dhe politikat publike.[55] E thënë ndryshe krimi teknologjik, kibernetik është i shtrirë pothuajse në të gjitha fushat ku këto mund të aplikohen dhe dëmet janë të pallogaritshme, përsa kohë çdo ditë e më tepër jeta e zakonshme e njerëzve po 'dixhitalizohet'.
- Ndikimi i teknologjisë në kryerjen e veprave penale fillon nga individi i thjeshtë deri tek qeveritë, shtrirja e saj nuk ka më përmasa kohore, gjeografike dhe shpejtësia me të cilën zhvillohen teknologjitë është propabilitet, për të qenë shumë shpejt i shfrytëzueshëm për t'u përdorur për sjellje devijante kriminale.

53 How Computers Are Used to Help Commit Crimes: https://www.hg.org/legal-articles/how-computers-are-used-to-help-commit-crimes-40716

54 Combating Computer Crime https://www.hg.org/legal-articles/combating-computer-crime-31034

55 Criminal Use of Technology, Richard K. Moule, https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0211.xml

- Nga ky kontekst i gjerë konstatojmë se nevojitet një bashkëpunim mjaft i ngushtë, koherent i të gjithë shteteve sovrane të harmoniozojnë legjislacionet e tyre të brendshme dhe të lehtësojnë procesin e ndihmës së ndërsjelltë ku shumicën e raste këto lloj krimesh kibernetike i tejkalojnë kufijt shtetëror.
- Ndërsa në vemendje të vendit tonë, përpos ndjekjes së vazhdueshme të standardeve ndërkombëtare, nevojitet një investim më i madh në kapitalin njerëzor të ekspertëve të teknologjisë, të rëndësishëm në struktuarat dhe mekanizmat qe ne kemi për mbikëqyrjen e zbatueshmërisë së ligjit kundër krimeve kibernetike, të hetimit të provave, të parandalimit të kryrjes së veprave penale përmes teknologjisë. Thënë kjo për të patur një drejtësi penale efektive.

Kjo shkon paralel me nevojën për trajnimin e vazhdueshëm edhe të policisë gjyqësore, prokurorëve dhe gjyqtarëve të cilët janë zbatuesit e ligjit dhe përgjegjësit më pas për efektshmërinë e luftimit të krimit kibernetik.

Bibliografia

Legjislacion, Raporte, Strategji, Artikuj

- Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001
- The Budapest Convention and its Protocols
- Kodi Penal
- Ligj Nr. 8888, datë 25.4.2002 Për Ratifikimin e "Konventës për Krimin në Fushën e Kibernetikës"
- Ligj Nr. 9262, datë 29.7. 2004, Për Ratifikimin e "Protokollit Shtesë Të Konventës Për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të Kryera Nëpërmjet Sistemeve Kompjuterike"
- Report On Cybersecurity Maturity Level in Albania, 2018
- Deeksha Sharma and Manik Dhingra, *"Technology, crime and its changing patterns*", Law Audience Journal, December 2018;
- Perkins, S., "How Technology has Changed Crime";
- Richard K. Moule, "Criminal Use of Technology";
- Articles by Lawyers, "How Computers Are Used to Help Commit Crimes

- Leksioni i Justice Breyer mbi të Drejtën Ndërkombëtare
- Europol Unclassified – Basic Protection Leve, Crime in the age of technology, The Hague, 12/10/2017, Përditësuar: 15.03.2022
- Përdorimi i ndihmës së ndërsjellë juridike Traktatet (Mutual Legal Assistance Treaties (MLAT) për t'u përmirësuar; Përgjimi i ligjshëm ndërkufitar; Procedurat, 12 September 2012
- Raporti Statistikor Mujor i Ministrisë së Brendshme Mars 2021, Analiza e Krimeve Kompjuterik
- Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025, Fletorja zyrtare. Nr.7, 2021

Praktika e GjEDNj

- Çështja S. dhe Marper kundër Mbretërisë së Bashkuar, 4 dhjetor 2008 (Dhoma e Madhe)
- Çështja Gaughran kundër Mbretërisë së Bashkuar, 13 shkurt 2020,
- Çështja Shimovolos kundër Rusisë, 21 qershor 2011
- Çështja Bernh Larsen Holding As dhe të tjerët kundër Norvegjisë
- Çështja Ivashchenko kundër Rusisë, 14 mars 2013

Burime online

https://www.lawaudience.com/technology-crime-and-its-changing-patterns/#google_vignette

https://study.com/academy/lesson/how-technology-has-changed-crime.html

https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0211.xml

https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html

https://www.hg.org/legal-articles/how-computers-are-used-to-help-commit-crimes-40716

https://study.com/academy/lesson/technocrime-forms-examples.html

https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_

the_age_of_technology_.pdf

https://www.hg.org/legal-articles/combating-computer-crime-31034

https://f3magazine.unicri.it/?p=310

https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

https://www.icc-portugal.com/images/publicacoes/documentos_gratuitos/Economia_Digital/ICC_policy_statement_on_Using_Mutual_Legal_Assistance_Treaties_(MLATs)_To_Improve_Cross-Border_Lawful_Intercept_Procedures_(2012).pdf

https://www.brookings.edu/blog/techtank/2017/04/21/as-criminals-adapt-to-new-technology-so-must-international-law/

https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

https://www.pp.gov.al/rc/doc/Raporti_Vjetor_Kuvendit_per_Kriminalitetin_2021_31_03_22_PP_6411.pdf

TEKNOLOGJIA DHE KRIMINALITETI: ROLI I KARTAVE TE KREDITIT

DR. IV ROKAJ LL.M
DR. TEUTA HOXHA

HYRJE

Rritja e përdorimit të kartave të kreditit për pagesat "business to business" (B2B) apo edhe përdorimin e përditshëm nga individë të ndryshëm, ka pasur një rritje shumë të madhe vitet e fundit. Sipas studimeve, këto shpenzime u rritën me 25%, nga 196 miliardë dollarë në 450 miliardë, me një parashikim për 10% rritje në vitin 2022. Përdorim masiv u rrit sidomos në kohën e pandemisë Covid-19, ku gjithcka u zhvillua me blerjet në distancë.Korriku 2022 shënon afërsisht dy vite e disa muaj që kur pandemia e koronavirusit u shfaq dhe nxiti shumë konsumatorë të kalojnë në modalitetin e bllokimit, pasi COVID-19 u përhap me shpejtësi dhe shumë konsumatorë u dyndën në internet për të blerë artikujt e tyre thelbësorë, duke i rritur shitjet elektronike në mënyrë eksponenciale.

Tregtia elektronike po rritej me shpejtësi përpara se të godiste COVID-19, por pandemia shtyu edhe më shumë konsumatorët qe të shpenzojnë më shumë në internet dhe më shpesh. Digital Commerce 360[1] vlerëson se pandemia kontribuoi përfundimisht me 218.53 miliardë dollarë shtesë në tregtinë elektronike gjatë dy viteve të fundit dhe në vitin 2020, koronavirusi shtoi 102.08 miliardë dollarë në tregtinë elektronike në SHBA dhe shtoi 116.45 miliardë dollarë në vitin 2021.

Në përgjithësi në vitin 2021, konsumatorët shpenzuan 870.78 miliardë

1 https://www.digitalcommerce360.com

dollarë në internet me tregtarët amerikanë, 14.2% më shumë nga 762.68 miliardë dollarë në vitin 2020. Nëse pandemia nuk do të kishte ndodhur, Digital Commerce 360 vlerëson se shitjet e tregtisë elektronike nuk do të kishin arritur në 820.78 miliardë dollarë për dy vitet e tjera dhe shitjet në internet do të kishin arritur vetëm 754.33 miliardë dollarë në 2021. Në këtëdrejtim kartat e kreditit luajnë një rol të dosmsdoshem.

Përfshirja e krimit të organizuar në krime financiare apo pastrim parash në sektorin e kartave të kreditit është ende një fushë e panjohur sot, megjithëse përdorimi i tyre në jetën e përditshme është gjithnjë e më i përhapur.

Organizatat kriminale po bëhen gjithnjë e më kreative me përdorimin e kartave të kreditit për të krijuar skema mashtruese apo krime të tjera financiare si dhe për lëvizjen e fondeve të paligjshme përtej kufirit pa rënë në sy të sistemeve rregullatore të aktivizuara për depozitat e parave dhe transfertat elektronike bankare.

Ky punim synon të analizojë lidhjen midis kartave të kreditit dhe teknologjisë, kryesisht duke e parë teknologjinë si një mjet parandalimi dhe luftimi të këtij fenomeni relativisht të ri kriminal dhe ekonomiko-financiar. Studimet e fundit tregojnë se metodat klasike të rregullave tëparacaktuara nga bankat si filtër detektues, tashmë janëjo efektive ndaj zbulimit tëkriminalitetit nëpërmjet kartave, për shkak të shpejtësisë, shpeshtësisë dhe elaborimit te tyre.

Ky punim synon të ofrojë një pasqyrë të qartë tësituatës se ku ka qenë dhe ku synon të shkoj lufta kundër kriminalitetit financiar nëpermjet kartave të kreditit, duke pasur parasysh inovacionin e serviur nga teknologjia.

Gjithashtu, duke qenë se ka pasur relativisht pak studime në këtë fushë, duke shqyrtuar sa më shumë shembuj të përdorimit të teknologjisë për lehtësimin e flukseve të paligjshme financiare, kjo analizë kërkon të ofrojë një kontekst për studime të mëtejshme në këtë fushë.

Kartat e kreditit dhe historiku i tyre

Një kartë krediti është një dokument plastik me një shirit sigurie dhe çip, i lëshuar nga një ent bankar ose financiar, i cili përdoret për të bërë blerje produktesh ose shërbimesh. Paratë e marra hua nga përdoruesi, institucioni lëshues financiar, i kërkon t'i kthehen me një vlerë interesi shtesë të përcaktuar më parë.

Karta e kreditit është pasardhëse e një sërë skemash krediti midis tregtarëve. Ajo u përdor për herë të parë në vitet 1920[2], në Shtetet e Bashkuara, për të shitur në mënyrë specifike karburant te një numer në rritje të pronarëve të automjeteve. Në vitin 1938 disa kompani filluan të pranonin kartat e njëra-tjetrës. Western Union[3] kishte filluar lëshimin e kartave të pagesës për klientët e saj të shpeshtë në vitin 1921, por"kartelat tarifore"me letërfalsifikoheshin lehtësisht.Koncepti i klientëve që paguajnë tregtarë të ndryshëm duke përdorur të njëjtën kartë u shpjegua në vitin 1950 nga Ralph Schneider dhe Frank McNamara, themeluesit e Diners Club[4], për të eliminuar kartat e shumta. Megjithëse kartat e kreditit arritën nivele shumë të larta të adoptimit në SHBA, Kanada dhe Mbreterinë e Bashkuar, ku në mesin e shekullit të njëzet, shumë kultura ishin më të orientuara nga paratë e gatshme ose zhvilluan forma alternative të pagesave pa para, të tilla si Carte Bleue[5] ose Karta Euro[6]. Vetë dizajni i kartës së kreditit është bërë një pikë kryesore e shitjes në vitet e fundit, ndërsa vlera e kartës për emetuesin shpesh lidhet me përdorimin e kartës nga klienti, me vlerën financiare të klientit.

Sipas Hill Dictionary karta e kreditit është një "identifikim i kartës që i mundëson mbajtësit të blejë mallra dhe shërbime në të tashmen dhe të paguajë për to në të ardhmen".

Sipas Peter Salim"një kartë krediti është një kartë e lëshuar nga një bankë ose institucion financiar për abonimin e tyre dhe për të mundësuar blerjen e mallrave dhe shërbimeve".

Kështu, karta e kreditit është një kartë e lëshuar nga një bankë ose

---

2 Artificial Intelligent Credit Risk Prediction: An Empirical Study of Analytical Artificial Intelligence Tools for Credit Risk Prediction in a Digital Era Diederick van Thiel AdviceRobo Tilburg University Ë. Fred van Raaij Tilburg University

3 Kompani e cila merret me tranferat e parave në kohë reale në të gjithë botën nëpërmjet pikave të saj.

4 Diners Club filloi historinë e tij në vitin 1950, e gjitha sepse një burrë i quajtur Frank McNamara darkoi në një restorant në Nju Jork, por i la paratë e tij në një kostum tjetër. Në pamundësi për të paguar faturën pa ardhur gruaja e tij për ta shpëtuar, ai vendosi të mos vinte më kurrë në siklet dhe themeloi Diners Club.
Tani, Diners Club International Ltd. është një kompani shërbimesh bankare dhe pagesash të drejtpërdrejta në pronësi të Discover Financial Services (NYSE: DFS), një nga markat më të njohura në shërbimet financiare të SHBA. Si një anëtar i Discover® Global Network, ai ka aftësitë për t'iu përshtatur nevojave tuaja. Ne ofrojmë një sërë opsionesh pagese, përfitimesh dhe oferta ekskluzive - në partneritet me tregtarë, restorante dhe marka kryesore të industrisë së shërbimeve në mbarë botë

5 LLoj karte krediti e quajtur karta blu

6 Lloj karte krediti e zhvilluar ne Europe pas daljes së monedhës euro

institucion tjetër financiar, ku pronari i kartës në një transaksion mund të marrë mallra ose shërbime duke treguar një kartë që mund të shërbejë edhe si mjet pagese me para në dorë.

Kartat e kreditit janë një pjesë themelore e rritjes ekonomike dhe tregtare të vendeve në zhvillim dhe të zhvilluara, pasi këto karta lejojnë transferimin e parave në internet, gjë që kontribuon në një mënyrë të përshpejtuar në zgjerimin dhe shpejtësinë e transfertave financiaresi dhe tregtisë elektronike.

Kredia është një metodë e shitjes së mallrave ose shërbimeve pa pasur para në dorë blerësi. Një kartë kreditiështë vetëm një mënyrë automatike për t'i ofruar kredikonsumatorit. Sot, çdo kartë krediti mbart njënumri identifikues që përshpejton blerjet dhetransaksionet. Sipas Enciklopedisë Britannica, përdorimi i kartave të kreditit e ka origjinën nëShtetet e Bashkuara gjatë viteve 1920, ku kompanitë e naftës dhe zinxhirët e hoteleve,filluan t'i lëshonin ato për klientët. Megjithatë,referenca për kartat e kreditit janë bërë që në vitin 1890 në Evropë. Kartat e hershme të kredititpërfshijnë shitjet drejtpërdrejtëdhe ndërmjet tregtaritduke ofruar kartën e kreditit si mënyrë pagese. Rreth vitit 1938, kompanitëfilluan të pranojnë kartat e njëri-tjetrit.

Në Evropë, karta krediti më e njohur kompanitë janë ndoshta Barclaycard, Citibank dheAmerican Express, duke ofruar lloje të ndryshmeproduktesh në varësi të portofolit të tyre. Në varësitë produktit të ofruar, shërbimet e lidhurame kartën mund të jenë të ndryshme. Norma e interesit, tarifat e kartës, tarifa e kursit të këmbimit, tarifa e vonesës së pagesës, kufiri i kredisë dhe termat dhe kushtet, janë elementë që mundndryshojnë nga një bankë në tjetrën dhe nga njëprodukt në tjetrin.

Megjithatë, duke qenë se është një metodë shumë e dobishme dhe e thjeshtë pagese, ajo u jep kryesve të veprave penale lehtësinë për të kryër vepra penale financiare të shumëllojshme.

Përbën domosdoshmëri sot, në kuadër të përparimeveteknologjikë në llogaritje, për të nxitur dhe krijuar mjete që lejojnë zbulimin dhe parashikimin e ketyre krimeve financiare përpara se të kryhen. Kompanitë si Platforma FICO (Falcon Fraud Manager)[7], ofrojnë shërbime për të menaxhuar dhe parandaluar mashtrimin. Kjo kompani përdor analizën e të dhënave dhe inteligjencën artificiale në këtë drejtim, e cila do të analizohet më tej në këtë punim.

7 FICO (NYSE: FICO) është një kompani lider softuerësh analitikë, që ndihmon bizneset në 90+ vende të marrin vendime më të mira që nxisin nivele më të larta rritjeje, përfitimi dhe kënaqësie të klientit.

Prodhuesit dhe emetuesit janë shumë pak sot, pavarësisht kohës së gjatë që nga krijimi i kartave apo faktit se mbas cilit emër tregëtar ato lëshohen.

Sot, me zgjerimin e e-commerce, më shumë se gjysma e të gjitha mashtrimeve të kryera bëhen nëpërmjet kartavetëkreditit dhe zakonisht mashtruesit kanë lidhje mebiznesin e prekur. Kryesishtmund të jetë një palë e brendshme, por ka shumë të ngjarë të jetë edhe një pale e jashtme, dukë u shfaqur sinjëklient i mundshëm/ekzistues ose furnizues i mundshëm/ekzistues.

Shumë kompani ndonjëherë kanë të bëjnë me miliona palë të jashtme dhe është një kosto shumë e madhe të kontrolloj manualisht shumicën e palëve të jashtme, përidentitetin dhe aktivitetin e tyre. Në të vërtetë, për të hetuar secilintransaksion të dyshimtë, këto kompani kanënjë shpenzim të drejtpërdrejtë mbi të ardhurat e tyre. Nëse shuma e një transaksioniështë më e vogël se kostoja e shpenzimeve të përgjithshme,hetimi nuk ia vlen financiarisht edhe sikur të duketi dyshimtë[8].

Problematika e gjetur

Transformimi i teknologjisë po i jep një pamje më të mirë çdo sektori, përfshirë shërbimet financiare. Megjithatë, dixhitalizimi i shpejtë është një thikë me dy tehe pasi kriminelët po sofistikohen dhe po eksplorojnë dobësitë e sigurisë dhe shmangin zbulimin për të lëvizur paratë e pista nëpër sistemet bankare. Vlerësohet se deri në 2 trilion dollarë pastrohen çdo vit, ekuivalente me pothuajse 5% të PBB-së[9] globale.

Pasojat e krimeve financiare janë shkatërruese dhe kanë një ndikim më të gjerë ekonomik, nësiguri dhe në aspektin social. Ato u lejojnë autorëve të aktiviteteve të paligjshme si trafikimi i qënieve njerëzore dhe narkotikëve dhe krimi i organizuar të vazhdojnë dhe zgjerojnë operacionet e tyre, duke shkaktuar humbje katastrofike për viktimat dhe duke shkaktuar kërdi në shoqëri. Aktivitete të tilla si financimi i terrorizmit përbëjnë një kërcënim të

8 Chan et al., 1999; Oscherëitz, 2005.

9 Një mënyrë për të matur zhvillimin e prosperitetit në shoqëri është vlerësimi i aktivitetit ekonomik. Mënyra më e përdorur për vlerësimin e fuqisë dhe performancës së një ekonomie është Prodhimi i Brendshëm Bruto (PBB). PBB-ja është vlera totale e të gjithë mallrave dhe shërbimeve që janë prodhuar në vend minus vlerën e mallrave dhe shërbimeve të nevojshme për prodhimin e tyre.
PBB-ja për frymë është gjithashtu një tregues i rëndësishëm i performancës ekonomike dhe një njësi e dobishme për të bërë krahasime të standardeve mesatare të jetesës dhe mirëqenies ekonomike. Prodhimi i Brendshëm Bruto (PBB) për frymë matet si raporti i PBB me numrin e popullsisë totale të atij vendi.

rëndësishëm për sigurinë kombëtare, duke e bërë këtë një kërcënim serioz për botën në përgjithësi.

Institucionet financiare po shpenzojnë kolektivisht miliarda dollarë duke u përpjekur të parandalojnë krimin financiar. Në vitin 2020, institucionet financiare në të gjithë botën kanë paguar 10.6 miliardë dollarë gjoba kundër pastrimit të parave (AML)[10]. Incidente të tilla krijojnë rreziqe komerciale dhe në reputacionin e institucioneve financiare. Pavarësisht të gjitha përpjekjeve, vetëm një pjesë e krimit financiar është identifikuar.

Korrupsioni, evazioni fiskal, krimi i organizuar, tregtia e drogës dhe trafikimi i qënieve njerëzore, si dhe flukset e paligjshme financiare të lidhura me këto aktivitete të paligjshme,paraqesin kërcënime të rëndësishme të ndërlidhura për shtetet. Ato reduktojnë ndjeshëm burimet e brendshme tashmë të kufizuara në dispozicion dhe ulin të ardhurat tatimore që nevojiten për të financuar programet dhe infrastrukturën kritike për uljen e varfërisë[11]. Në mënyrë indirekte, ato gjithashtu ndikojnë negativisht në investime, nxitin inflacionin e tepërt që çon në norma më të larta interesi, lehtësojnë krijimin e ekonomive të paqëndrueshme, kërcënojnë sigurinë, nxisin pabarazinë, si dhe minojnë sundimin e ligjit. Këto shqetësime rritën presionin nga shoqëria civile dhe aktorë të tjerë për të ndërmarrë veprime kundër flukseve të paligjshme financiare.

Çështja e flukseve të paligjshme financiare nuk është e re; megjithatë, në dekadat e fundit varësia në rritje e shoqërisë nga rrjetet e informacionit dhe komunikimit po ndryshojnë peizazhin e këtij problemi. Rritja e operacioneve dixhitale në tregjet legjitime është një nga shtytësit me kritikë për zhvillimin ekonomik. Megjithatë, ndërsa tregjet dhe tregtia kanë tërhequr gjithmonë kriminelët që kërkojnë përfitime nga aktivitetet e paligjshme, rrjetet dixhitale kanë kriuar mundësi kyçe për format e reja të transferimit të fondeve të paligjshme dhe një lehtësimin në shumë mënyra të sistemeve tradicionale të flukseve të paligjshme financiare. Aktiviteti kriminal ka evoluar paralelisht me përdorimin e rrjeteve të informacionit nga shoqëria, duke reaguar ndaj çdo zhvillimi teknologjik me qasje të reja për të përfituar dhe fshehur ato. Natyra pa kufijë dhe arkitektura e decentralizuar e internetit, e kombinuar me një ekosistem kompleks dinamik të ekonomisë dixhitale, paraqet sfida të reja për qeveritë, industrinë dhe shoqërinë civile në trajtimin e problemit të flukseve të paligjshme financiare, kundër lehtësuesit më të mëdhenj janë

10 Anti Money Laundering ose ndryshe AML simbolizon një akronim i cili përdoret gjërësisht për të definuar luftën, iniciativat, sektoret dhe ligjet kunder pastrimit te parave.

11 Banka Botërore 2015.

edhe kartat e kreditit

Për shkak të risive relative të problemit, ka ende mungesë të hulumtimit për çështjen e teknologjive dixhitale si mundësues dhe lehtësues i flukseve të paligjshme financiare, ashtu sikur ka akoma më shumë mangësi në studime serioze të cilat adresojnë zgjidhje efikase nëpermjet përdorimit të teknologjisë dhe inteligjencës artificiale në luftën kundër veprave penale të keyera nëpermjet përdorimit të kartave të kreditit.

Gjithashtu, rritja e llojeve të kartave dhe fleksibiliteti i tyre rrit rriskun, sepse sa më i madh dhe masiv përdorimi, aq më i vështirë detektimi. Metoda klasike e rregullave të paracaktuara nga bankat tashmë janëjo efektive ndaj zbulimit të veprave penale nëpërmjet përdorimit të kartave.

Flukset e paligjshme financiare janëtashmë një çështje ndërsektoriale në axhendën ndërkombëtare të viteve të fundit. Fondet e paligjshme nga krimi i organizuar, korrupsioni dhe evazioni fiscal, të cilat lëvizin përtej kufijve, përbëjnë një sfidë të madhe për sigurinë dhe stabilitetin e ekonomive anembanë globit, me një efekt veçanërisht shkatërrues për vendet në zhvillim. Nuk ka vlerësime të besueshme të flukseve financiare të paligjshme. Sipas disa vlerësimeve, afro 1 trilion dollarë fonde të paligjshme zhvendosen çdo vit nga tregjet në zhvillim dhe vendet në zhvillim[12]. Megjithatë, nuk ka asnjë provë të besueshmërisë së vlerësimeve të tilla.

Në ditët e para të krimit kibernetik, skena dominohej kryesisht nga individë ose grupe hakerësh të lidhur që kryenin sulme vetëm për argëtim ose për të demonstruar aftësitë e tyre teknike[13]. Zhvillimi dhe rritja e ekonomisë dixhitale ndryshoi në mënyrë dramatike si peizazhin kriminal ashtu edhe motivimin e shkelësve, duke e transformuar krimin e lidhur me kibernetikën në një industri kriminale komplekse dhe të lulëzuar. Ashtu si në rastin e flukseve të paligjshme financiare në përgjithësi, nuk ka vlerësime të besueshme mbi fitimet kriminale dhe humbjet në imazh, si dhe kostot e rikuperimit që mund të shkojnë shumë përtej dëmit të drejtpërdrejtë. Shumica e vlerësimeve vijnë nga kompanitë e sigurisë kibernetike, kështu që po vihen në dyshim në lidhje me besueshmërinë e statistikave të krimit dhe vlerësimet e humbjeve[14]. Megjithatë, pasiguria për fitimet dhe humbjet nga krimi për bizneset nuk do të thotë se nuk ka një kuptim të përgjithshëm se fitimet kriminale dhe humbjet direkte dhe indirekte për bizneset janë shumë të larta.

12 Global Financial Integrity 2014; ONE 2014.

13 SecureWorks 2010.

14 Jardine 2015.

Megjithëse objektivat kryesore të kriminelëve kibernetikë janë vendet e zhvilluara më të pasura të cilat kanë një përdorim masiv të kartave të kreditit dhe varen shumë nga teknologjia e informacionit, mendohet se shumë krime e kanë origjinën në vendet e Azisë, Afrikës dhe Evropës Lindore[15], kjo e lidhur edhe me faktin që vendi i kryerjes së veprës penale me pozicionin gjeografik të keqbërësit nërastet e ketyre krimeve, mund të jenë të ndryshëm.

Zhvillimi i industrisë së krimit kibernetik nxitet nga vlerat monetare e të dhënave dhe shërbimeve të tregtuara në platformat specifike të internetit dhe nëpërmjet kanaleve të komunikimit, të cilat përdoren si tregje nëntokësore[16].

Kriminaliteti në internet përfshin një spektër të gjerë te aktivitetit ekonomik të fragmentuar dhe shumë të specializuar, ku aftësitë dhe të dhënat që ofrohen për shitje përbehen nga grupe të ndryshme kriminale të cilat specializohen në zhvillimin e mjeteve specifike të shkrimit të kodit për softuer me qëllimin e kryerjes së veprave penale në këtë fushe.

Ekonomia e fshehtë po strukturon operacionet e saj duke kopjuar modele biznesi nga sektorë legjitimë.

Ky punim synon të ofrojë një pasqyrë të qartë të situatës se ku ka qenë dhe ku synon të shkoj lufta kundër kriminalitetit financiar nëpërmjet kartave të kreditit, duke pasur parasysh inovacionin e servirur nga teknologjia.

Gjithashtu, duke qenë se ka pasur relativisht pak studime në këtë fushë, duke shqyrtuar sa më shumë shembuj të përdorimit të teknologjisë për lehtësimin e flukseve të paligjshme financiare, kjo analizë kërkon të ofrojë një kontekst për studime të mëtejshme në këtë fushë.

Memdime dhe sugjerime per te ardhmen e kesaj “lufte”

Të nxitur nga dixhitalizimi global i stileve të jetesës, bota aktualisht po përjeton një shpërthim të të dhënave të “sjelljes”[17]. Transmetimet e klikimeve, historitë e transaksioneve, mediat sociale, sondazhet psikografike ofrojnë volume të mëdha të të dhënave të sjelljes[18]. Aplikacione të reja për vendimmarrjen e kreditoreve janë duke u zhvilluar. Shumë familje në vendet në zhvillim nuk kanë histori financiare formale, duke e bërë të vështirë për bankat dhënien e kredive dhe për huamarrësit e mundshëm marrjen e tyre.

15 Europol 2015.

16 Europol 2014; Fallmann et al. 2010.

17 Van Thiel, et.al., 2017.

18 Me sjellje në këtë rast do të nënkuptojmë historikun e plotë te mënyrës, formës, shpështësisë, histrorikut të veprimtarisë ekonomike dhe sociale të një individi.

Megjithatë, shumë nga këto familje kanë telefona celularë, të cilët gjenerojnë të dhëna të pasura për sjelljen e tyre në përgjithësi.

Björkegren dhe Grissen argumentojnë se "nënshkrimet e sjelljes" në të dhënat e telefonit celular parashikojnë mospagimin e kredisë, duke përdorur të dhënat e thirrjeve, të cilat duhet të përputhen me rezultatet e huasë[19]. Van Thiel & Van Raaij analizojnë se tiparet psikografike që ofrojnë njohuri në qëndrimet, stilet e jetesës dhe vlerave, parashikojnëangazhimin e klientit[20].

Sjellja sociale dhe gjuha e një personi mund të pasqyrojnë karakteristikat e sjelljes së tyre, të cilat mund të përdoren si të dhëna krediti. Në internet, sjellja dhe gjuha e përdoruesve mund të merren nga mediat sociale. Një numër gjithnjë e më i madh burimesh të dhënash me karakteristika potencialisht më klasifikuese dhe parashikuese do të pasojnë në vitet e ardhshme.

Çdo ditë krijohen 2.5 kuintilion bajtë[21] të dhëna dhe 90% e të dhënave në botë sot janë prodhuar tashmë brenda viteve të kaluara[22]. Aftësia jonë për gjenerimin e të dhënave nuk ka qenë kurrë kaq e fuqishme dhe e madhe që nga zbulimi i"Teknologjisë së Informacionit"në fillim të shekullit të 19-të[23].

Meqenëse shumica e këtyre të dhënave të reja janë të pastrukturuara, kërkohen modele të reja analitike që mund të përballojnë të dhënat e strukturuara dhe të pastrukturuara. Nëfundin e viteve 1980, algoritme të ndryshme të "nxjerrjes" së të dhënave janë zhvilluar nga studiues të komunitetet të inteligjencës artificiale bazuar në alegoritmet dhe bazën e të dhënave. Shumica e këtyre algoritmeve[24] të njohura si nxjerres së të dhënave janë inkorporuar në sistemet komerciale dhe jane të hapura të "minierat e të dhënave"[25] Përparime të tjera, të tilla si rrjetet nervore për klasifikimin/ parashikimin dhe grupimin përdoren si algoritme gjenetike për optimizimin dhe mësimin e makinerive, duke kontribuar në suksesin e nxjerrjes së të

19 Björkegren, et.al., 2018

20 Van Thiel, et.al., 2017

21 Björkegren, D., & Grissen, D. (2018). Behavior revealed in mobile phone usage predicts loan repayment. Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A. Ë., & Siddique, A. (2016). Risk and risk management in the credit card industry Journal of Banking and Finance, 72, 218-239.

22 IBM, 2016.

23 Wu, et.al., 2014.

24 Algoritmi në matematike dhe informatikë, është një veprim i përcaktuar saktë për zgjidhjen e një problemi ose të një lloji të caktuar problemesh. Algoritmi mund të përkufizohet si një *ecuri* që lejon të fitohet një *rezultat* i dhënë duke ndjekur, në një renditje të përcaktuar, një tërësi *hapash të thjeshtë* që përkojne me veprimet e zgjedhura nga një tërësi e kufizuar. Algoritmi pra, është ecuria që krijon përgjigjen për një pyetje, çështje ose zgjidhjen e një problemi me një numër të kufizuar hapash.

25 Databaza shumë të mëdha me të dhëna

dhënave në aplikacione të ndryshme[26].

Në fakt, proçesi fillon me një hap me të avancuar të para-përpunimit të të dhënave, ku një gamë e gjerë mjetesh të mësimit të makinerive përdoren për të përmirësuar cilësinë e të dhënave. Proçesi përfshin imputimin e të dhënave, ku është i rëndësishëm filtrimi i të dhënave për të dhëna shumë të rralla, dhe zbulimi dhe menaxhimin e të dhënave të jashtme për ato më pak sensitive. Zgjedhja e teknikave të përdorura i lihet modeluesit, me mundësinë për të vizualizuar efektin në kohë reale të metodave të përdorura në grupin e të dhënave.

Pikerisht në këtë prizëm na vjen në ndihmë edhe në këtë sektor përdorimi i teknologjisë AI[27] (Inteligjenca Artificiale), e cila ka një impakt të madh në luftën kundër krimeve financiare nëpërmjet përdorimit të kartave të kreditit. Ky hap i rëndësishëm teknologjik përdor algoritme të sofistikura të cilat arrijnë të parandalojnë kryerjen e krimeve financiare nëpermjet kartave duke aplikuar profilizime të ngjashme me "cookie"[28] që përdor Google etj, për të krijuar një profil të qartë të përdoruesit dhe aplikuar në mënyre thuajse parandaluese standartet e njih "Klientin Tënd" nga banka lëshuese apo banka transmetuese të transanksionit.

Kompanitë po përdorin inteligjencën artificiale për të parandaluar dhe zbuluar gjithçka, nga vjedhjet rutinë të punonjësve të tyre deri tek tregëtia në përgjithësi. Shumë banka dhe korporata të mëdha përdorin inteligjencën artificiale për të zbuluar dhe parandaluar mashtrimin dhe pastrimin e parave.

---

26 Chen, et.al., 2012.

27 Inteligjenca artificiale (IA) i referohet aftësisë së një kompjuteri për të kryer funksione dhe arsyetime që aktualisht janë tipike vetëm të mendjes njerëzore. Shpesh termi i referohet edhe degës së shkencës kompjuterike që ka për qëllim krijimin e saj. Tekstet e librave përkufizojnë këtë fushë si "studimi dhe krijimi i agjentëve inteligjent ku një agjent inteligjent është një sistem që e percepton mjedisin e tij dhe merr masa për të maksimizuar shanset e tij për sukses. John McCarthy, i cili solli termin më 1956,e përkufizon si "shkenca dhe inxhinieria e bërjes së makinave inteligjente.

28 Cookie është informacion i ruajtur në pajisjen tuaj nga faqja e internetit që po viziton. Cookies zakonisht ruan cilësimet, cilësimet për faqen në internet si dhe gjuhën dhe adresën e preferuar. Më vonë, kur të hapni përsëri faqen, shfletuesi do t'i dërgojë këta cookies mbrapsht. Kjo mundëson që faqja të tregojë informacione të përshtatura për nevojat tuaja, sepse faqja web i kujton veprimet tuaja në një periudhë të caktuar kohore. Çdo herë që hapni faqe, shfletuesi do të lexojë vlerat e ruajtura në cookie.
Cookies mund të kenë një gamë të gjerë informacionesh përfshirë informacionin personal (emri, mbiemri, email). Megjithatë, ky informacion do të përdoret vetëm nëse ju jepni leje për të - faqja e internetit nuk mund të ketë informacione që nuk i keni dhënë dhe nuk mund të ketë akses në pajisjen tuaj. Megjithatë, mund ta ndryshoni konfigurimin e shfletuesit tuaj në një mënyrë për të zgjedhur personalisht nëse do të miratoni ruajtjen e cookies ose jo, për të fshirë të gjitha cookies kur mbyllni shfletuesin etj. Gjithashtu, nëse jepni lejen tuaj për përdorimin e cookies-ve, gjithashtu mund ta tërhiqni atë.

Kompanitë e mediave sociale përdorin AI për të bllokuar përmbajtjet e paligjshme si pornografia e fëmijëve apo komentet bullizuese, rraciste apo të zbulojnë dhe heqin videot dhe mesazhet e rekrutimit terrorist ne ëeb[29] pothuajse menjëherë etj. Bizneset po eksperimentojnë vazhdimisht me mënyra të reja për të përdorur inteligjencën artificiale për një menaxhim më të mirë të rrezikut dhe zbulim më të shpejtë dhe më të përgjegjshëm të mashtrimit, madje edhe për të parashikuar dhe parandaluar krimet.

Ndërsa teknologjia bazë e sotme nuk është domosdoshmërisht revolucionare, algoritmet dhe rezultatet që ajo mund të prodhojnë janë, për shembull, bankat kanë përdorur për dekada sisteme të monitorimit të transaksioneve të bazuara në rregulla binare të paracaktuara qëkërkojnë me pas nje kontroll manual. Shkalla e suksesit është përgjithësisht e ulët: Mesatarisht, vetëm 2% e transaksioneve të shënuara nga sistemet pasqyrojnë përfundimisht një krim të vërtetë ose qëllim kriminale. Sot makineritë po përdorin rregulla parashikuese që njohin automatikisht anomalitë në grupet e të dhënave. Këto algoritme të avancuara mund të zvogëlojnë ndjeshëm numrin e sinjalizimeve të rreme duke filtruar rastet që janë shënuar gabimisht, ndërsa zbulojnë raste të tjerat të humbura, duke përdorur rregulla konvencionale.

Duke pasur parasysh pasurinë e të dhënave të disponueshme sot dhe pritshmëritë në rritje të klientëve dhe autoriteteve publike, kur bëhet fjalë për mbrojtjen dhe menaxhimin e atyre të dhënave, shumë kompani kanë vendosur që AI është një nga mënyrat e vetme për të vazhduar luftën në mënyrë të suksesshme kundër krimeve financiare të cilat nga ana e tyre bëhen gjithnjë e më të sofistikuar.

Përcaktimi nëse zgjidhja e luftimit të krimit me anëtë AI është një zgjidhje e përshtatshme për një kompani zgjidhetnëse përfitimet i tejkalojnë rreziqet që i shoqërojnë ato. Një rrezik i tillë qëndron në rastin kur mund të nxirren përfundime të njëanshme bazuar në AI, duke përdorur faktorë si përkatësia etnike, gjinia dhe mosha. Kompanitë gjithashtu mund të përjetojnë reagime të kundërta nga klientët që shqetësohen se të dhënat e tyre do të keqpërdoren ose shfrytëzohen nga një mbikëqyrje edhe më intensive e të dhënave, transaksioneve dhe komunikimeve të tyre, veçanërisht nëse këto njohuri

29 World Wide Web (shkurt WWW ose the Web; Rrjeti gjithë botërorë) është një hapësirë informacioni ku dokumentet dhe burimet e tjera të internetit identifikohen nga Uniform Resource Locators (URLs), të ndërthurura nga lidhjet hypertext, dhe mund të arrihen nëpërmjet internetit. Shkencëtari anglez Tim Berners-Lee krijoi Ëorld Ëide Ëeb në vitin 1989. Ai shkroi programin kompjuterik të shfletuesit të parë në vitin 1990 derisa ishte i punësuar në CERN në Zvicër. Shfletuesi u publikua jashtë CERN-it në vitin 1991, së pari në institucione të tjera kërkimore që filluan në janar 1991 dhe në publikun e gjerë në internet në gusht të vitit 1991.

ndahen me qeverinë.

Kohët e fundit, për shembull, një bankë evropiane u detyrua të tërhiqej nga plani i saj për t'u kërkuar klientëve leje për të monitoruar llogaritë e tyre të mediave sociale si pjesë e procesit të aplikimit të tyre për kredi, pas një proteste publike mbi taktikat e saj te modelit "Big Brother".Përpara se të nisin një iniciativë për menaxhimin e rrezikut të AI, menaxherët duhet së pari të kuptojnë se ku mësimi i makinerive tashmë po bën një ndryshim të madh.

Megjitahtë bankat, për shembull, po i ndalojnë krimet financiare shumë më shpejt dhe më lirë sesa dikur, duke përdorur AI për automatizimin e proceseve dhe kryerjen e analizave shumështresore të "mësimit të thelluar". Edhe pse bankat tani depozitojnë 20 herë më shumë raporte të aktiviteteve të dyshimta të lidhura me pastrimin e parave sesa në vitin 2012, mjetet e inteligjencës artificiale i kanë lejuar ato të zvogëlojnë "ushtrinë e njerëzve" që punësojnë për të vlerësuar alarmet për aktivitetet e dyshimta. Kjo për shkak se sinjalizimet e tyre të rreme kanë rënë përgjysmë falë AI, dhe sepse shumë banka tani janë në gjendje të automatizojnë punën rutinë të ligjeve njerëzore në vlerësimin e dokumenteve[30]. Për shembull, duke përdorur inteligjencën artificiale, Paypal[31] gjithashtu ka përgjysmuar alarmet e rreme.

Gjithashtu, mjetet AI lejojnë kompanitë të shfaqin modele ose marrëdhënie të dyshimta të padukshme edhe për ekspertët. Për shembull, rrjetet nervore artificiale mund t'u mundësojnë punonjësve të parashikojnë lëvizjet e radhës edhe të kriminelëve të paidentifikuar, të cilët kanë gjetur mënyra për të shmangur alarmet e sistemeve binare të sigurisë të bazuara në rregullat konvencionale. Këto rrjete nervore artificiale lidhin miliona pika të dhënash nga bazat e të dhënave, në dukje të palidhura që përmbajnë gjithçka, nga postimet e mediave sociale deri te adresat e protokolleve të internetit të përdorura në rrjetet Wi-Fi të aeroporteve, si dhe pronat e pasuritë e paluajtshme, tatim-taksat etj.

Kompanitë dhe agjencitë e zbatimit të ligjit kanë eksperimentuar veçmas me përdorimin e inteligjencës artificiale për të përmirësuar aftësinë e tyre për të zbuluar dhe parandaluar krimin. Tani, ata po punojnë gjithnjë e më shumë së bashku duke zhvilluar platforma të përbashkëta të të dhënave, protokolle

30 Application of Artificial Intelligence (Artificial Neural Network) to Assess Credit Risk: A Predictive Model For Credit Card Scoring-Samsul Islam University of Auckland.

31 PayPal është mënyrë e sigurt dhe e lehtë për të paguar dhe për t'u paguar në internet. Shërbimi i lejon këdo që të paguajë në çfarëdo mënyre që ai preferon, duke përfshirë përmes kartave të kreditit, llogarive bankare, PayPal Smart Connect ose gjendjeve të llogarive, pa shkëmbyer informacion financiar.

raportimi etj. Partneritetet publiko-private për të luftuar krimin do të bëhen gjithnjë e më të zakonshme. Institucionet financiare, njësitë e inteligjencës financiare dhe zbatimi i ligjit kanë filluar të krijojnë partneritete publike-private për të shkëmbyer të dhëna dhe për të përdorur AI për të zbuluar krimin në juridiksione të caktuara. Për shembull, në Mbretërinë e Bashkuar, Agjencia Kombëtare e Krimit po punon ngushtë me Financat e Mbretërisë së Bashkuar për të përdorur AI në mënyrë që të identifikojë më mirë jo vetëm krimin financiar dhe ekonomik, por gjithashtu të përmirësojë aftësinë e tyre për të përdorur informacionin financiar për të zbuluar lloje të tjera krimesh si trafikimi i qenieve njerëzore dhe falsifikimit, etj.

Autoritetet po kërkojnë gjithashtu gjithnjë e më shumë mënyra për të rritur shkëmbimin e informacionit dhe inteligjencës ndërmjet sektorit publik dhe atij privat.

Ndërsa krimi i organizuar dhe kriminelët bëhen më të sofistikuar dhe sasia e të dhënave të disponueshme për sektorin privat vazhdon të rritet në mënyrë eksponenciale, kompanitë dhe organet ligjzbatuese do të krijojnë edhe më shumë në partneritete publiko-private për të shfrytëzuar pasurinë e të dhënave qe kane në zotërim dhe për të zbuluar aktivitetet e mundshme kriminale edhe më me efikasitet.

Gjithashtu,AInë sektorin financiar është vendosur fillimisht si pjesë e programit të pajtueshmërisë me AML[32] të bankave apo institucioneve te tjera financiare dhe përfaqëson një seri algoritmesh që kontrollojnë masat dixhitale të vendosura për të zbuluar pastrimin e parave, krimet financiare (dhe aktivitete të tjera kriminale). Këto algoritme në këtë rast, analizojnë sasi të mëdha të të dhënave të klientit, duke përfshirë kujdesin e duhur ndaj klientit, kontrollin e sanksioneve dhe inputet e monitorimit të transaksioneve, për të kryer një sërë detyrash të automatizuara, thuajse parandualuese dhe "parashikuese" të sjelljeve në mënyrë që të detektohet aktiviteti i dyshimtë.

Aplikimi i mësimit të makinerive AI brenda një infrastrukture të AI-se, do të thotë që programet AML, mund të bëhen edhe më efikase. Duke përdorur të dhënat e monitorimit të transaksioneve të analizuara më parë, mjetet e mësimit të makinerive mund të vlerësojnë sjelljen e klientëve në zhvillim dhe të bëjnë një përcaktim më të saktë për nivelin e rrezikut të pastrimit të parave që sjell sjellja.

AI jo vetem kryen detyrat më shpejt se një oficer i kontrolli i AML-në, por, nëpërmjet mësimit të makinerive, ka aftësinë të përshtatet me kërcënimet e

32 Do Digital Technologies Facilitate Illicit Financial Flows? Dr. Tatiana Tropina.

reja dhe metodologjitë e reja të pastrimit të parave, duke siguruar që firmat të jenë në gjendje të ripozicionohen shpejt në mjedise të ndryshme rregullatore dhe te qëndrojne një hap përpara kriminelëve.

Përtej krijimit të profileve të rrezikut të klientëve, pajtueshmëria me AML kërkon analizën e të dhënave të pastrukturuara si pjesë e monitorimit të transaksioneve. Për të vlerësuar siç duhet rrezikun që ata paraqesin klientët, firmat duhet të përpiqen t'i përdorin ato të dhëna për të kuptuar jetën e tyre sociale, profesionale dhe politike, duke shqyrtuar një sërë burimesh të jashtme dhe duke përfshirë mediat dhe arkivat publike, rrjetet sociale dhe grupe të tjera të dhënash përkatëse.

Inteligjenca artificiale mund të ndihmojë raportimin e aktiviteteve të dyshimtajo vetëm duke gjeneruar raportet automatikisht, por duke i plotësuar ato automatikisht me informacionin përkatës. Nëpërmjet standardizimit të gjuhës dhe terminologjisë dhe duke rritur kështu fokusin për zbatueshmërinë e rregulloreve, AI jo vetëm që mund të rrisë shpejtësinë dhe efikasitetin e raportimit të AML të një kompanie, por edhe ndikimin e saj në hetimet e mëvonshme nga autoritetet.

AI mund t'i ndihmojë kompanitë të krijojnë një pasqyrë më të pasur për klientët dhe modelet e transaksioneve, duke i lejuar ato të eliminojnë sinjalizimet e pasakta dhe të parëndësishme që e bëjnë proçesin e detektimit aq të kushtueshëm për kompanitë dhe të vështirë për klientët.

Megjithatë, miratimi i AI ka ende një rrugë të gjatë perpara. Për shumicën e bankave dhe institucioneve financiare, udhëtimi sapo ka filluar ose nuk ka filluar ende.

Për fat të mirë, shpjegueshmëria në rritje e sistemeve të AI do të ndihmojë në ndërtimin e besimit të përdoruesit në përdorimin e AI. Kjo, së bashku me mbështetjen rregullatore që shohim për përdorimin e AI në AML, përfundimisht do të inkurajojë dhe mbështesë adoptimin e kësaj teknologjie në këtë sector kaq të rëndësishëm për shoqërinë.

Ndër të tjera, përdorimi i AI në grupe të ndryshme të dhënash, ka si sfidë kryesore ruajtjen e besimit. Institucionet publike dhe ato private nuk mund të funksionojnë pa besimin e palëve të tyre të interesit dhe të shoqërisë në përgjithësi. Zbulimi, parandalimi dhe denimi i krimit financiar është një gur themeli i këtij besimi, por metodat e zbulimit të përdorura duhet të jenë në përputhje me vlerat tona morale dhe të drejtës tonë për privacy dhe për të gëzuar një jetë të qetë, si një ndër parimet më themelore kushtetuese.

Një nga efektet e mundshme negative të përdorimit të AI në këtë sektor është

mbështetja në vendimet e marra pa ndërveprim njerëzor, gjë që ndërlikon llogaridhënien brenda një institucioni. Kush është përgjegjës, duke qenë se një algoritëm nuk mund të jetë përgjegjës më vete? Gjithashtu, algoritmet duhet të dizajnohen dhe trajnohen me shumë kujdes për të shmangurrezultate te padëshirueshme. Të gjithë duartrokasin zero tolerancë për kriminelët, por shoqëria ka më pak se zero tolerancë për softuerin AI që mundte kriminalizoj njerëzit e pafajshëm.

Bashkimi Europian paraqet disa parime kyçe që AI të jetë i besueshëm[33].

Së pari, privatësia dhe rujtja e të dhënave është një e drejtë e njeriut që duhet të merret parasysh në proçeset e zbulimit të krimit financiar, si kudo tjetër. Ligjet e privatësisë përmbajnë në mënyrë eksplicite dispozita për të bërë të mundur përdorimin e të dhënave, për sa kohë që ato janë proporcionale dhe ekzistojnë masa adekuate mbrojtëse. Gjithashtu është rëndësishme të kontrollohet nëse ka mjete të tjera, më pak të rënda, për të arritur këto objektiva.

Së dyti, shpjegueshmërianë lidhje me sistemet e AI mund të jenë aq komplekse saqë të kuptuarit se si arrihet një vendimarrje bëhet pothuajse e pamundur, e njohur ndryshe si fenomeni i "kutisë së zezë"[34].

Së treti, transparenca për të ditur kur dhe ku sistemet e AI janë duke u vendosur brenda një zinxhiri vendimmarrës. Kur zbulohet krimi financiar me AI, profesionistët njerëzorë duhet të jenë gjithmonë në ciklin e proçesit të vendimmarrjes, me aftësinë për të ndryshuar ose anuluar vendimet nëse është e nevojshme dhe për më tepër, njerëzit e prekur nga vendimet duhet të kenë akses në ankimim e dëmshpërblim për çdo vendim të automatizuar që merret ndaj tyre në lidhje me krimin financiar, të cilat janë marrë në mënyrë të gabuar dhe nuk figurojnësi të tilla.

LITERATURA

- A Comprehensive Survey on Machine Learning Techniques and User Authentication Approaches for Credit Card Fraud Detection, Niloofar Yousefi, Marie Alaghband, Ivan Garibay Department of Industrial Engineering and Management Systems University of Central Florida Orlando, Florida, USA

33 Explain Artificial Intelligence for Credit Risk Management-DELOITTE.

34 Një pajisje elektronike zakonisht e komplikuar, mekanizmi i brendshëm i së cilës është zakonisht i fshehur ose misterioz për përdoruesit.

- A machine learning based credit card fraud detection using the GA algorithm for feature selection-Emmanuel Ileberi, Yanxia Sun Zenghui Wang
- Alejandro Correa Bahnsen, Aleksandar Stojanovic, Djamila Aouada, and Bjorn Ottersten. Cost sensitive credit card fraud detection using bayes minimum risk. In Proceedings-2013 12th In- ternational Conference on Machine Learning and Applications, ICMLA 2013, volume 1, pages 333–338. IEEE Computer Society, 2013.
- Application of Artificial Intelligence (Artificial Neural Network) to Assess Credit Risk: A Predictive Model For Credit Card Scoring-Samsul Islam University of Auckland.
- Artificial Intelligent Credit Risk Prediction: An Empirical Study of Analytical Artificial Intelligence Tools for Credit Risk Prediction in a Digital Era Diederick van Thiel AdviceRobo Tilburg University W. Fred van Raaij Tilburg University.
- Björkegren, D., & Grissen, D. (2018). Behavior revealed in mobile phone usage predicts loan repayment. Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A. Ë., & Siddique, A. (2016). Risk and risk management in the credit card industry Journal of Banking and Finance, 72, 218-239.
- Changjun Jiang, Jiahui Song, Guanjun Liu, Lutao Zheng, and Wenjing Luan. Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 2018.
- Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy" published by IEEE Transactions on Neural Netëorks and Learning Systems, vol. 29, No. 8, August 2018.
- Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi" published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.
- CREDIT CARD FRAUD DETECTOR USING ARTIFICIAL INTELLIGENCE, Luis Zhinin-Vera, March 2020.
- DeNardis. 2015. "Internet Architecture as Proxy for State Poëer." In IP Justice Journal: Internet Governance and Online Freedom Publication Series.

- Do Digital Technologies Facilitate Illicit Financial Flows? Dr. Tatiana Tropina.
- Explain Artificial Intelligence for Credit Risk Management- DELOITTE.
- FRAUD DETECTION IN CREDIT CARD SYSTEM WEB MINING- Hetvi Modi, Shivangi Lakhani, Nimesh Patel, Vaishali Patel,
- International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013.
- Khandani, A. E., Kim, A. J., & Lo, A. Ë. (2010)- Consumer credit-risk models via machine-learning algorithms, Journal of Banking and Finance, 34 (11), 2767-2787.
- Kodi Penal i Republikës së Shqipërisë.
- Leonard K. 1995 - The development of a rule based expert system model for fraud alert in consumer credit'-European Journal of Operational Research.
- Ligji Nr.9917, datë 19.5.2008 "PËR PARANDALIMIN E PASTRIMIT TË PARAVE DHE FINANCIMIT TË TERRORIZMIT", i ndryshuar.
- RENEWAL OF CRIMINAL LAË AGAINST ABUSE OF CREDIT CARDS- Eka Nugraha, Syukri Akub, Badriyah Rifai, Marthen Arie, Hasanuddin University Graduate
- The Credit Card and the Crimes Associated with It-Bassam Mustafa Tubishat& Khaldoun Faëzi Kandah.
- The modus operandi of perpetrators for credit card fraud in the Vaal Region, South Africa-Witness Maluleke, Moses Morero Motseki, Rakgetse John Mokëena & Siyanda Dlamini.
- The Use of Technology to Combat Identity Theft-Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003, February 2005.
- Wheeler, R. & Aitken, S. 2000-'Multiple Algorithms for Fraud Detection', Knowledge-Based Systems.

TECHNOLOGICAL DEVELOPMENT, IMPACT ON HUMAN RIGHTS AND FREEDOMS

PH.D. SAFET KRASNIQI
University " Ukshin Hoti" Prizren / safet.krasniqi@uni-prizren.com

Ph.D. MIRVETE UKAJ
Radio Television of Kosovo / mirveteuka@rtklive.com

RILIND HOTI
Student at the University "Ukshin Hoti" in Prizren / rilindhoti99@gmail.com

Abstract

The paper will address the importance of technical-technological development in the digital age, the direct impact on our social life and the dangers that may arise during use. These risks are related to the need to protect human rights and freedoms in national and international legislation. The purpose of this paper is the challenges that are being overcome by state authorities and various international organizations in terms of human rights, except the positive aspect related to human health. Drafting a general strategy in the field of judicial and police cooperation between countries as a result of the increase in the number of technological crimes, are the key factors that enable cooperation between countries. While science and technology are advancing rapidly on the other hand we have setbacks in terms of drafting and enforcing legislation as a factual and legal protector of human rights and freedoms. The question arises as to what needs to be done to overcome the challenges posed by technological development in relation to human rights and freedoms? States in their positive legislations need to be more

determined in the face of the development of technology that is spiraling out of control. National and international legal systems do not yet have complete legislation that would provide full legal protection to those individuals who could face the risk that technology poses to their rights and freedoms. During this paper will be analyzed concrete cases, which have been the subject of review by the Strasbourg court. Research, analysis, comparison, historical methods were used.

Keywords: Technology, human rights and freedoms, technological development, interstate cooperation, Strasbourg Court.

Epoka Digjitale

Mënyra e zhvillimit të jetës sociale në përgjithësi, ka pësuar ndryshime në epokën digjitale. Këtij ndryshimi i ka paraprirë revolucioni industrial, e tashmë vetëm në këtë epokë të zhvillimit tekniko-teknologjik shoqëria njerëzore e ka mundësinë që të gëzojë këto ndryshime[1]. Epoka digjitale karakterizohet kryesisht me tendencën e lehtësimit të punës, mirëqenies të njeriut, aksesit në informacione dhe njohuri që ishin të kufizuar për njerëzit në përgjithësi. Nëse flasim për këtë epokë, mund të i referohemi edhe si "epoka e informacionit", për shkak se informacioni është faktori kryesor që i'u intereson të gjithëve dhe mundohen ta kenë të gjithë. Informata në përgjithësi në këtë erë bartet shumë shpejtë, sakaq edhe ka bërë që zhvillimi teknologjisë të jetë dukshëm më i madh me krahasim me epokat tjera. Pikërisht këtu qëndron epërsia e kësaj epoke që në fakt edhe po tejkalon pritjet e zhvillimit të teknologjisë duke i'u referuar gjithmonë ndihmës të Intelegjencës Artificiale(IA). Intelgjenca Artificiale si faktor në këtë epokë është thelbësor në çdo aspekt. Njeriu gjithmonë ka shtyer limitet e tij duke krijuar dhe zhvilluar teknologji të reja, por tani ka krijuar edhe Intelegjencën Artificiale që në fakt mundet të i shërbejë shumë në zhvillimin dhe krijimin e këtyre teknologjive. Një teknologji si Intelegjenca Artificiale mund të i ofrojë njerëzimit mundësi më të mira në kohë reale, duke i kursyer kohë dhe mund. Por prap mbetet teknologji që mundet edhe të shfrytëzohet edhe për anë negative dhe mund të krijojë pasoja të pa riparueshme në të ardhmen.

1 https://dzone.com/articles/the-digital-age-the-era-we-all-are-living-in-and-d, qasur më 5 korrik 2022.

Përkufizimi i Intelegjencës Artificiale

Para se të fokusohemi në aspektin njerëzor, e që drejtpërdrejt lidhet me të drejtat e njeriut dhe mbrojtjen e këtyre të drejtave nga rreziqet që vijnë nga përparimi i inteligjencës artificiale, janë përkufizimet dhe definicionet lidhur me inteligjencën artificiale. Prej shumë definicioneve, më të rëndësishmet janë definicioni i Komitetit të Parlamentit Evropian dhe definicioni standard. Komiteti i Parlamentit Evropian për Çështjet Ligjore, e përcakton Inteligjencën artificiale si një robot të zgjuar që fiton autonomi përmes sensorëve, ose duke shkëmbyer të dhëna me mjedisin e tij. Ajo shkëmben dhe analizon të dhëna, ka një mbështetje fizike dhe përshtat sjelljet dhe veprimet e tij me mjedisin[2]. Sipas përkufizimit standard inteligjenca artificiale nënkupton një makinë, kompjuter dhe softuer, që përmban një shkallë inteligjence të atillë me inteligjencën njerëzore dhe që e lejon atë të funksionojë dhe të reagojë si njerëzit madje, në të ardhmen e saj edhe me reagim emocional. Sistemet e inteligjencës artificiale, shfaqin sjellje të ngjashme me inteligjencën njerëzore, të tilla si: planifikimi; të mësuarit; arsyetimi; zgjidhja e problemeve; përpunimi i njohurive; perceptimi; lëvizja; inteligjenca sociale dhe krijimtaria.[3] Në anën tjetër, zgjidhja e problemeve, veçanërisht në inteligjencën artificiale, mund të karakterizohet si një kërkim sistematik përmes një sërë veprimesh të mundshme për të arritur një qëllim ose zgjidhje të paracaktuar.[4]

Inteligjenca Artificiale në syrin e analizave kritike

Përparimi i madh tekniko-teknologjik në botën bashkëkohore, përpos avantazheve sjell edhe rreziqe për njeriun, posaçërisht në të ardhmen afatgjate. Pasojat e saj, godasin direkt individin. Jeta dinamike dhe zhvillimi i hovshëm ka bërë që njeriu të "distancohet" nga bashkëshortësia dhe bashkëpunimi e komunikimi shoqëror, ndër individual e kolektiv. Parashikimet janë të frikshme për shume shtete, veçanërisht për shtetet ku IA, tanimë ka zënë vend në jetën zhvillimore. Analizat e ekspertëve të ndryshëm parashikojnë që duke filluar nga 2030, popullata e Koresë së Jugut dhe Japonisë, do të jetojnë në një "bashkëjetesë" robot – njeri, sikundër që parashikohet që të

2 EPRS | European Parliamentary Research Service,2020, e qasëshme https://dig.watch/updates/ai-features-european-parliaments-legal-affairs-committee-discussion, qasur më 3 nëntor 2021.

3 Nick Heath, 2021,What is AI? Here's everything you need to know about artificial intelligence, e qasëshme në https://www.zdnet.com/article/what-is-ai-everything-you-need-to-know-about-artificial-intelligence,. qasur 4 nëntor 2021.

4 https://www.britannica.com/technology/artificial-intelligence, qasur më 14 korrik 2022.

ligjësohet martesa e njeriut me robot5. Po ashtu, garën e armatimit bërthamor e cila zhvillohej dikur, tani po e zëvendëson gara në armatim në sfondin e inteligjencës artificiale. Komisioni i Sigurisë i SHBA-së për Inteligjencën Artificiale tregon se, bëhet fjalë për një paradigmë të re të të luftuarit, në të cilën, përballja "algoritmet kundër algoritmeve" ka për qëllim garën, për të qenë vazhdimisht më novator se kundërshtari. Plani i fundit pesëvjeçar i Kinës, vendos në qendër të vëmendjes hulumtimin dhe zhvillimin, ndërsa Ushtria Popullore Kineze armatoset për një të ardhme, sikurse e quan ajo "të luftës së bazuar tek inteligjenca". Ka mjaft shtete të cilat janë duke u munduar në këtë garë edhe pse nuk janë fuqi të mëdha ushtarake. Shembull për këtë janë edhe dronët vrasës të cilët u përdorën në luftën e vitit 2020 në mes të Azerbejxhanit dhe Armenisë për Nagornjikarahun, "Loitering Munition", të quajtur si "dronë kamikaz". Përdorimi i armëve të shkatërrimit me pasoja kolektive për njerëzimin, bie ndesh me Konventën për Armët e Caktuara Konvencionale" të OKB-së, e vlefshme nga viti 1983. Konventa synon të kontrollojë armët që "shkaktojnë vuajtje të panevojshme dhe të pajustifikueshme" e që ndryshe quhen edhe armë të shkatërrimit në masë6.

Mbrojtja e të drejtave të njeriut sipas Deklaratës Universale për të Drejtat e Njeriut dhe KEDLNJ

Njohja e dinjitetit, që u përket të gjithë anëtarëve të shoqërisë njerëzore, si edhe njohja e të drejtave të tyre të barabarta dhe të patjetërsueshme, përbënë themelin e lirisë, drejtësisë dhe paqes në botë. Kjo është përcaktuar në Deklaratën Universale për të Drejtat e Njeriut dhe Konventën Evropiane për të Drejtat dhe Liritë e Njeriut(KEDLNJ) dhe konsiderohet si pikënisja e orientimit juridik e politik në rrafshin e mbrojtjes juridike të të drejtave të njeriut. Të gjithë njerëzit janë të barabartë para ligjit dhe kanë të drejtë pa asnjë diskriminim, të mbrohen barabartë nga ligji. Të gjithë kanë të drejtën për t'u mbrojtur barabar kundër çdo diskriminimi që cenon këto dokumente, si dhe kundër çdo nxitje për një diskriminim të tillë. Është pikërisht neni-7 i Deklaratës i cili fakton barabarësinë juridike të garantimit të të drejtave dhe lirive të njeriut[7]. Në jetën tonë të përditshme, duke u nisur nga të thënat dhe

5 Danielle Muoio , ,2015, This researcher has an interesting theory for why robots need legal rights, qasur më 25 tetor 2021, e qasëshme në https://www.businessinsider.com/yueh-hsuan-weng-explains-why-robots-need-legal-rights-2015-11,

6 https://www.dw.com, qasur më 28 tetor 2021.

7 Deklarata Universale për të Drejtat e Njeriut (DUDNj) u miratua nga Asambleja e Përgjithshme e Kombeve të Bashkuara më 10 dhjetor 1948 në Palais de Chaillot të Parisit. Kjo deklaratë

të dhënat e sipër cekura, shumë herë jemi subjekte të nxitjes, por edhe të shkeljes së të drejtave njerëzore, tani edhe përmes formave moderne teknologjike, siç është Facebook dhe rrjetet tjera sociale, të cilat përmes postimit të lajmeve algoritmike nxitën jo vetëm diskriminim por edhe dhunë si pasojë e gjuhës së urrejtjes. Ka mendime dhe deklarata të shkencëtarëve por edhe të politikanëve të ndryshëm të cilët kanë mendim Pro et Contra. Ata që janë të mendimit se zhvillimi i inteligjencës artificiale, krahas të mirave që i sjell njeriut, kufizon të drejtat e njeriut marrin shembull lajmet algoritmike. Rasti i nxitjes së dhunës në Mianmar është shembulli më i saktë i argumentimit të tyre[8], ose e ashtuquajtura "Kredi Sociale" që e aplikon Kina. Sistemi ka funksione ndëshkuese, të tilla si "ndëshkimi" i debitorëve, nëpërmjet shfaqjes së fytyrave të tyre në ekrane të mëdha në hapësirat publike ose duke i vendosur këta individë në "listën e zezë" në udhëtimet me tren ose avion[9]. Nisur nga këto dhe shembuj të tjerë, mendojnë se një zgjidhje do të ishte përfshirja e Deklaratës Universale të OKB-së për të Drejtat e Njeriut në gjuhën e programimit të inteligjencës artificiale. Ish-Ambasadorja e Shteteve të Bashkuara në Këshillin e OKB-së për të Drejtat e Njeriut, Eileen Donahoe, ka deklaruar se duhet të merren për bazë normative aktuale, dokumentet ndërkombëtare për të drejtat e njeriut. Të tjerët nuk pajtohen me konstatime të tilla. Ish anëtarja e Parlamentit Evropian, Marietje Schaake, duke bërë krahasime në mes të ideologjisë së sotme globale, pra të demokracisë apo shtetit ligjor të quajtur ndryshe, thekson se përpos sfidave tjera jetësore të njeriut që paraqiten sot për shkak të dinamikës jetësore, por edhe interneti i ditëve të sotme, nuk vijnë prej teprisë së rregullave, por prej mungesës së rregullave për teknologjinë. Megjithatë, ekspertët janë të pajtimit se është i domosdoshëm një rregullator global që do të sigurojë praktikat etike të inteligjencës artificiale. Eric Schmidt, kreu i Komisionit të Sigurisë Kombëtare të SHBA-ve për Inteligjencën Artificiale, thekson nevojën imediate se sistemi që po ndërtohet në epokën moderne, duhet të bazohet në vlerat njerëzore pasi që, megjithatë, inteligjenca artificiale është shpikur nga njeriu dhe i shërben vetëm njeriut[10]. Shumë ekspertë të

ishte si reaksion i pasojave të luftës së dytë botërore. Deklarata ishte përpjekje për të ligjësuar mbrojtjen e të drejtave themelore të njeriut të cilat të drejta, pa dallim, ju takojnë të gjithëve. Neni 7 i Deklaratës thekson barabarësinë e të gjithëve para ligjit, pa asnjë lloj diskriminimi pa dallim.

8 https://www.reuters.com/investigates/special-report/myanmar-facebook-hate., qasur më 14 korrik 2022.

9 China's Social Credit System puts its people under pressure to be model citizens2018,e qasëshme në https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963, qasja , 5 nëntor 2021.

10 Zëri i Amerikës, 13 dhjetor 2019.

Inteligjencës Artificiale(IA) besojnë se ky shekull do të dëshmojë krijimin e teknologjive, inteligjenca e të cilave e tejkalon atë te njerëzve në të gjitha aspektet. Qëllimet e tilla, në parim mund të marrin ndonjë formë të mundshme qe do të ndikojë në të ardhmen e planetit tonë, aq shumë sa që mund të paraqesin një rrezik ekzistencial për njerëzimin. Speciet tona dominojnë vetëm Tokën, duke qëndruar dhe mbi kafshët e tjera qe jetojnë në të, sepse aktualisht kanë nivelin më të lartë të inteligjencës. Por, është e besueshme se deri në fund të shekullit, do të jetë zhvilluar Inteligjenca Artificiale, einteligjencë e cila krahasohet me tonat. Për më tepër, nuk mund të përjashtohet mundësia që Inteligjenca Artificiale të zhvillojë edhe nivele fenomenale te vetë ndërgjegjes dhe në një të ardhme edhe mundësinë për të ndier dhimbje, të cilat do të na ballafaqojnë me lloje të reja të sfidave[11]. Shkencëtari Ray Kurzweil, autori i librit të famshëm "The singularity is near" ka thënë se progresi i gjithë shekullit XX, do të arrihet brenda vetëm 20 vjetëve të shekullit XXI-të. Sipas statistikave, në vitin 2000, ritmi i progresit ishte pesë herë më i shpejtë se progresi mesatar i gjithë shekullit XX-të. Nisur nga këto sfida, rritet rreziku për mundësinë e kufizimit të mëtejmë të të drejtave të njeriut siç janë: **liria e shprehjes, privatësia apo edhe të drejtat tjera civile.** E drejta për jetë pra, e drejta e secilit për ta zgjedhur mënyrën e të jetuarit, familja, personaliteti dhe e drejta në privatësi, janë të drejta që përkundër faktit se janë të parapara në dokumentet ndërkombëtare e që në kohët moderne janë bërë standarde ndërkombëtare, megjithatë, mund të paraqesin rrezik për kufizim apo edhe shkelje të këtyre të drejtave. Ky parashikim tani më është realitet dhe se ndryshimet janë aq të mëdha sa që deri në vitin 2030 dallimet në zhvillimin njerëzor, do t'i tejkalojnë parashikimet sa që do të mund të ndodhin aq shumë ndryshime dhe do të ketë zhvillime aq të mëdha, sa që ndryshimet do jenë marramendëse ndërmjet viteve 2018-2030[12]. Për më tepër, sapo kompjuterët mund të ri programojnë veten në mënyrë efektive dhe të përmirësojnë veten në mënyrë të njëpasnjëshme, duke çuar në një të ashtuquajtur "singularitet teknologjik" ose "shpërthim inteligjent", rreziqet e makinerive që tejkalojnë njerëzit në beteja për burime dhe vetë-ruajtje nuk mund të anashkalohen thjesht[13]. Sipas parashikimeve të Kurzweil, në vitin 2050 mund të ndodh singulariteti në teknologji e që i bie që zhvillimi i inteligjencës artificiale do të jetë aq i madh sa që do ta ndryshojë tërësisht civilizimin njerëzor. Bota, nga këto

11 IA, mundësi dhe sfida, https://sites.google.com/site/inteligjencaartificialeledion/ qasur më 5 nëntor 2021

12 Po aty, kapitulli 2, qasur më 30 tetor 2021

13 https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence, qasur më 14 korrik 2022.

ndryshime që do të mund të ndodhin, nuk do të mund të njihet. E përkundër të gjitha këtyre zhvillimeve, sërish do t'i referohemi Deklaratës Universale për të Drejtat e Njeriut, konkretisht nenit 12. Nga ky këndvështrim, familja, e drejta e banimit dhe pacenueshmëria e banesës, korrespondenca, personaliteti, nderi dhe prestigji i gjithë secilit, mbrohet nga ligji kundër ndërhyrjeve ose sulmeve të tilla. Shtetet kombëtare, janë duke u ballafaquar nga këto sfida në legjislacionet e tyre të brendshme duke qenë në mes të aspektit pozitiv të inteligjencës artificiale dhe rreziqeve që kjo sjell gjatë aplikimit të saj në jetën shoqërore, p.sh. në këndvështrim pozitiv, inteligjenca artificiale do të lejojë të dëmtuarit në shikim dhe të verbrit, të vrapojnë në mënyrë të pavarur. Sistemi është duke u testuar nga kompania Google dhe do të drejtojë përdoruesin përmes një aplikacioni në në telefon të mençur, përmes një pajisjeje që mund të shndërrohet në një lloj syri dhe veshi, që drejton rrugëtimin. Për të përdorur sistemin, përdoruesi duhet të lidhë një telefon Android me një "parzmore" e hartuar nga Google, që vendoset rreth belit. Aplikacioni "Project Guideline" do të përdorë kamerën e telefonit për të ndjekur rrugën. Po ashtu, shkencëtarët po e testojnë një sistem të inteligjencës artificiale, që mendohet se është i aftë që ta diagnostikojë demencën pas një skanimi të vetëm të etj[14]. Një aspekt negativ i zhvillimit të inteligjencës artificiale është ndikimi në të dhënat personale, përmes mbledhjes dhe analizimit të të cilave, mund të zbulohen informacione personale në lidhje me përdoruesit. Shumë shtete akoma janë larg pranimit të këtyre ndryshimeve dhe si të tilla edhe kanë ende mungesë legjislative. Në aspektin ekonomik në vitin 2011, Kombet e Bashkuara paraqitën Parimet Udhëzuese për Biznesin dhe të Drejtat e Njeriut, të cilat i bëjnë thirrje industrisë të respektojë, të mbrojë dhe të sigurojë instrumente mbrojtëse për të drejtat e njeriut. Komisionari i Këshillit të Evropës për të Drejtat e Njeriut argumentoi se në epokën e inteligjencës artificiale, e drejta e privatësisë, mos diskriminimit dhe liria e shprehjes, duhet të mbrohen në mënyrë të veçantë[15]. Nga aspekti krahasimor i dy Konventave ndërkombëtare për të drejtat e njeriut, ngjashmëritë dhe dallimet në raporte ndërmjet tyre dhe aspektin e mbrojtjes së të drejtave të njeriut nga ndikimet që ka IA. KEDLNJ, në nenet 8 dhe 10 të saj, jo vetëm që njeh, por garanton të drejtën për respektimin e jetës private dhe familjare dhe lirinë e shprehjes. Këto të drejta, janë potencialisht të rrezikuara për shkak të ndërhyrjeve, përgjimeve të ndryshme, me qëllim uljen e autoritetit personal të individit, gjithnjë me

14 Koha ditore, 1 Dhjetor 2019.

15 Euro News, Albania, Çfarë duhet të dini për strategjinë e re të BE për inteligjencën e artificiale,2020 e qasëshme në https://euronews.al/al/risi/2020/02/19/cfare-duhet-te-dini-per-strategjine-e-re-te-be-per-inteligjencen-e-artificiale, qasur më 06.11.2021.

cak, dominimin dhe përfitimet e ndryshme materiale, politike, personale etj. Kështu, në Shqipëri, në një databazë me të dhënat personale dhe sensitive të 637,183 qytetarëve u shpërnda në seri përmes aplikacionit "Whatsapp", duke shënuar rrjedhjen më të madhe të të dhënave zyrtare në këtë vend[16]. Lidhur me këto të drejta dhe liri, Parlamenti Evropian ka marrë iniciativë për marrjen e masave për shkak të menaxhimit të paligjshëm të veprimeve të internetit, në rast të mosveprimit për eliminimin e veprimeve të tilla[17].

Rastet e shqyrtuara nga Gjykata Evropiane e të Drejtave të Njeriut

Gjykata Evropiane e të Drejtave të Njeriut me seli në Strazburg në kuadër të juridiksionit të saj përfshin edhe trajtimin e rasteve që përbëjnë shkelje të të drejtave të njeriut në aspektin teknologjik. Më poshtë do marrim shembuj specifik që ka shqyrtuar dhe ka nxjerr aktgjykime kjo gjykatë.

Shembulli i parë është rasti i çështjes Shimovolos kundër Rusisë. Objekt i padisë është keqpërdorimi të dhënave personale për shkak të arrestimit dhe ndalimit të paligjshëm. Gjykata ka konstuar se përdorimi i të dhënave personale të Shinovolos, përbën shkelje të nenit 8 të KEDLNJ. Gjykata vërtetoi se mënyra e mbledhjes së të dhënave dhe përdorimi i këtyre të dhënave është bërë në kundërshtim me nenin e sipërcekur të Konventës. Ky vendim njëra nga shumë mënyrat e shkeljes së të drejtave dhe lirive themelore të njeriut nga organet shtetërore e që ka ndikim të veçantë ky zhvillimin i teknologjisë[18].

Rasti i tjetër çështja Bernh Larsen Holding As dhe të tjera kompani kundër Norvegjisë. Objekt i padisë ishte vendimi i autoriteteve tatimore ndaj ankesës ndaj tri kompanive norvegjeze sipas të cilit këto kompani obligoheshin që autoriteteve tatimore të i'u jepeshin nga një kopje e të gjitha të dhënave në një server kompjuteri i cili u përdor bashkarisht. Në server kishte masa

16 https://www.reporter.al/rrjedhja-e-pagave-te-630-mije-qytetareve-shkakton-skandal-ne-shqiperi/, qasur më 14 korrik 2022.

17 Konventa Evropiane për të Drejtat e Njeriut (KEDNj), nenet 8-10. Zyrtarisht, Konventa për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, hartuar në vitin 1950 nga Këshilli i Evropës. Konventa hyri në fuqi më 3 shtator 1953.

18 Chamber judgment in the case Shimovolos v. Russia (application no. 30194/09), Chamber judgment in the case Shimovolos v. Russia (application no. 30194/09), the European Court of Human Rights held, unanimously, that there had been: A violation of Articles 5 § 1 (right to liberty and security) and a violation of Article 8 (right to respect for private life) of the European Convention on Human Rights. E qasëshme në https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-3581541-4053078%22]}, qasur më 7 korrik 2022.

mbrojtëse kundër abuzimit eventual të dhënave. Gjykata konstatoi se nuk kishte shkelje të nenit 8 të KEDLNJ. Gjykata u pajtua me argumentitimin e gjykatave norvegjeze se ky vendim është marrë për arsye efikasiteti dhe autoritet tatimore nuk duhet të kufizohen për të vepruar. Kompanitë në serverin e tyre kishin përdorur arkivë të përzier që përmbanin të dhëna të taksapaguesve tjerë. Këto dy vendime janë shembulli më i qartë i ndikimeve që mund të ketë teknologjia digjitale qoftë në aspektin pozitv ose negativ[19].

Komisioni Evropian për Efikasitetin e Drejtësisë (KEED) erdhi me një qëndrim se në mënyrë të përgjegjshme në fushën e drejtësisë duhet të përdoret IA, ku domosdoshmërisht duhet të ketë përshtatje me të drejtat themelore të njeriut të garantuara, në veçanti me Konventën Europiane mbi të Drejtat e Njeriut (KEDNJ) dhe Konventën e Këshillit të Europës për Mbrojtjen e të Dhënave Personale. Për më tepër është thelbësore të sigurohet që IA të mbetet një mjet në shërbim të interesit të përgjithshëm dhe se përdorimi i saj respekton të drejtat individuale. Parimet kryesore që duhet të respektohen në fushën e AI janë:

- Parimi i respektimit të të drejtave themelore: sigurimi se zbatimi i mjeteve dhe shërbimeve të inteligjencës artificiale është në përputhje me të drejtat themelore;
- Parimi i mosdiskriminimit: veçanërisht parandalimi i çdo diskriminimi ndaj individëve ose grupeve të individëve;
- Parimi i cilësisë dhe sigurisë: në lidhje me përpunimin e vendimeve gjyqësore dhe të dhënave, duke përdorur burime të certifikuara dhe të dhëna të paprekshme, në një ambient të sigurt teknologjik;
- Parimi i transparencës, paanshmërisë dhe drejtësisë: duke i bërë metodat e përpunimit të të dhënave të kuptueshme, duke autorizuar auditimet e jashtme;
- Parimi ”përdoruesi e ka nën kontroll”: duke siguruar që përdoruesit janë aktorë të informuar dhe nën kontrollin e zgjedhjeve të tyre.[20]

19 Chamber judgment in the case of Bernh Larsen Holding As and Others v. Norway (application no. 24117/08), the European Court of Human Rights held, by a majority, that there had been: no violation of Article 8 (right to respect for private and family life, home and correspondence) of the European Convention on Human Rights. E qasëshme në https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:[%22003-3581541-4053078%22]%7D., qasur më 7 korik 2022.

20 https://www.eurospeak.al/news/aedini/14223-perdorimi-i-inteligjences-artificiale-ne-sistemet-gjyqesore/, qasur më 14 korrik 2022.

Prezantimi dhe analiza e rezultateve

Gjatë shqyrtimit të literaturës, jemi angazhuar sidomos në analizën që u kemi bërë dispozitave të Deklaratës Universale për të Drejtat e Njeriut, definicionet zyrtare te BE për IA dhe ndikimin e IA-së, në jetën tonë shoqërore. Në parim, shpikës dhe komandues i IA-së, është vet njeriu. Kjo nuk kontestohet por të kontestueshme janë pasojat që IA ka sot dhe në të ardhmen, tek njeriu. Deri më sot, ka shumë pak shtete dhe më shumështete në BE që kanë hartuar plan afatgjatë të vëzhgimit, analizimit dhe kontrollit të zbatimit të avancimit të IA. Edhe pse kjo normativë juridike është duke u hartuar e duke u përsosur çdo ditë, dobitë dhe rreziku nga IA janë duke shkuar paralel. Shembull tipik është truri i njeriut i cili është duke u analizuar në prizmin e funksionimit të tij, njëkohësisht është shpikur një rrjetë neutrale artificiale."Simulimi i tërësishëm i trurit" është tjetër eksperiment i cili synon që duke u skanuar çdo pjesë e trurit, është krijimi i një modeli 3D i cili futet në kompjuter e më pastaj edhe krijimi i një makine inteligjence e ngjashme me trurin tonë. Nga këto të thëna dhe të dhëna, çështja e zbatimit të dokumenteve juridike ndërkombëtare ose kombëtare vështirësohet edhe nëse ato hartohen dhe kjo ka të bëjë me dy faktorë:

a) IA është në duar të atyre që e kanë shpikur dhe

b) Të atyre që e administrojnë dhe e menaxhojnë

Duke pasur parasysh se IA e kufizuar dallon nga IA e përgjithshme dhe posaçërisht nga super inteligjenca artificiale, në pikëpamje zhvillimore, kjo na bën akoma më kurioz se si do të adresohen çështjet e ndryshme lidhur me të drejtat e njeriut, konkretisht, si do të merren vendimet gjyqësore, në procedurat të cilat lidhen direkt me diskriminim, cenim të lirisë së shprehjes, cenim të privatësisë etj. Pra, a ekziston rreziku qe të vihet në pikëpyetje dinjiteti njerëzor? Konventa Evropiane për të Drejtat dhe Liritë e Njeriut, ka barazuar në pikëpamje të mbrojtjes juridike të drejtave dhe lirive e njeriut, duke i vendosur në piedestalin më të lartë, pa bërë asnjë dallim. Në pikëpamje të mbrojtjes së të drejtave të njeriut nga cenimi i mundshëm si pasojë e veprimeve të IA, mbrojtja juridike e të drejtave të njeriut do të mund të bëhej përmes sanksionimit të këtyre shkeljeve, paraprakisht duke bërë identifikimin e tyre përmes krijimit të mekanizmave juridik e politik. Kjo mund të bëhet duke aktivizuar praktikat juridike ndërkombëtare të të drejtave të njeriut, sanksionet penale dhe dëmshpërblimet në raste të vërtetimit nga gjykata se ka ndodhur cenimi i të drejta.

Përfundime dhe rekomandime

Ritimi i zhvillimit në epokën digjitale ka mundësuar zhvillim të hovshëm të teknologjisë, duke tejkaluar pritshmëritë dhe duke mundësuar digjitalizimin e jetës shoqërore. Megjithatë njeriu është krijues dhe sajues i këtij digjitalizimi dhe duke pasur parasysh qenien e vet dhe domosdoshmërinë e ekzistimit, mbrojtja e dinjitetit njerëzor përmes institutcioneve shtetërore është po aq e nevojshme sa ky digjitalizim i jetës tonë. Kjo mbrojtje nga një rrezik i tillë bëhet duke siguruar zbatim të plotë të normave juridike qofshin ato në drejtat e brendshme pozitive ose në drejtën ndërkombëtare.

Pyetjes së parashtruar në fillim të punimit, se çfarë duhet të bërë në tejkalimin e sfidave të paraqitura përgjatë këtij zhvillimi teknologjik, ne rekomandojmë: Aftësimi dhe trajnimi, informimi dhe edukimin lidhur me rreziqet e teknologjisë dhe informacionit. Kjo nënkupton specializimin e gjykatësve dhe prokurorve me qëllim të aftësimit të tyre për zhvillimin e prcedurave gjyqësore dhe marrjen e vendimeve. Ky edukim dhe trajnimet e ndryshme duhet të bëhën nga organizatat dhe institutcionet e specializuara qofshin ato vendore ose ndërkombëtare. Në suaza të rekomandimeve duhet të theksohet edhe nevoja e bashkëpunimit me komunitetin në përgjithësi që ky komunitet të jetë i gatshëm të ofrojë ndihmë dhe informacione në kapjen e kryerësve të krimeve kibernetike në kuadër të bashkëpunimit komunitet-institutcion.

Burimet dhe Literatura

- Deklarata Universale për të Drejtat e Njeriut (DUDNj) u miratua nga Asambleja e Përgjithshme e Kombeve të Bashkuara më 10 dhjetor 1948 në Palais de Chaillot të Parisit.
- Konventa Evropiane për të Drejtat dhe Liritë e Njeriut, (KEDNj), emri zyrtar, Konventa për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore) Hartuar në vitin 1950, hyri në fuqi më 3 shtator 1953.
- Zëri i Amerikës, 13.12.2019
- Koha ditore, 1 Dhjetor 2019

https://dzone.com/articles/the-digital-age-the-era-we-all-are-living-in-and-d.

EPRS | European Parliamentary Research Service,2020, https://dig.watch/updates/ai-features-european-parliaments-legal-affairs-committee-

discussion.

Nick Heath, 2021,What is AI? Here's everything you need to know about artificial intelligence, https://www.zdnet.com/article/what-is-ai-everything-you-need-to-know-about-artificial-intelligence.

https://www.britannica.com/technology/artificial-intelligence

Danielle Muoio ,2015, This researcher has an interesting theory for why robots need legal rights,https://www.businessinsider.com/yueh-hsuan-weng-explains-why-robots-need-legal-rights-2015-11

https://www.dw.com

https://www.reuters.com/investigates/special-report/myanmar-facebook-hate.

China's Social Credit System puts its people under pressure to be model citizens2018,https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963,

https://sites.google.com/site/inteligjencaartificialeledion/

https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence

Euro News, Albania, Çfarë duhet të dini për strategjinë e re të BE për inteligjencën e artificiale,2020 https://euronews.al/al/risi/2020/02/19/cfare-duhet-te-dini-per-strategjine-e-re-te-be-per-inteligjencen-e-artificiale

https://www.reporter.al/rrjedhja-e-pagave-te-630-mije-qytetareve-shkakton-skandal-ne-shqiperi/

Chamber judgment in the case Shimovolos v. Russia (application no. 30194/09), Chamber judgment in the case Shimovolos v. Russia (application no. 30194/09), the European Court of Human Rights held, unanimously, that there had been: A violation of Articles 5 § 1 (right to liberty and security) and a violation of Article 8 (right to respect for private life) of the European Convention on Human Rights. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-3581541-4053078%22]}

Chamber judgment in the case of Bernh Larsen Holding As and Others v. Norway (application no. 24117/08), the European Court of Human Rights held, by a majority, that there had been: no violation of Article 8 (right to respect for private and family life, home and correspondence) of the European Convention on Human Rights. https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:[%22003-3581541-4053078%22]%7D.

https://www.eurospeak.al/news/aedini/14223-perdorimi-i-inteligjences-artificiale-ne-sistemet-gjyqesore/.

"DIGITAL PROFILING E CYBERCRIME, LA NUOVA FRONTIERA DEL CRIMINE"

Ph.D. Av. ENIDA BOZHEKU (Ph.D. Avv.)

Capo Dipartimento "Pubblico e Privato", Collegio Universitario "Qiriazi", Tirana, Albania

Avvocato presso l'Ordine degli Avvocati di Roma

Avvocato presso l'Ordine degli Avvocati di Tirana

enida.bozheku@qiriazi.edu.al

Abstract

Con l'avvento della tecnologia anche il mondo del crimine si e' evoluto ed adattato a questa nuova dimensione di commissione dei reati. In particolar modo il cybercrime si sta sviluppando a ritmi elevati con un impatto sociale non indifferente. Internet e le varie piattaforme sociali stanno avendo un ruolo particolarmente incisvo sul mondo del crimine, dove, si rileva un elevato livello di crimini in aree come l'e-banking, l'e-commerce, il syberbullismo, la pedopornografia online, le truffe o addirittura il riclaggio di danaro e/o ricettazione.

Da qui, sembra chiaro che il ruolo degli investigatori sia davero decisivo nel combattere tali fenomeni criminali. Infatti la specializzazione degli agenti investigativi in ambito di cybercrime e di digital profiling sembra essere di fondamentale necessita'.

L'evolversi della teconoligia, dunque, porta anche l'evolversi del crimine. Da un punto di vista soggettivo esso inquadra le caratteristiche prorpie dei soggetti agenti, ossia del reo, il quale psicologicamente dimostra di essere un soggetto con capacita' criminali evolute, piu' flessibili, e molto accurate nei dettagli.

La difficolta' della tracciabilita' del luogo da cui si commettono i reati online, rappresenta un altro profilo problematico, in quanto gli agenti investigativi devono escogitare livelli di tracciabilita' "in rete" atti a identificare il luogo da cui il reo agisce e le peculiarita' psicologiche che esso utilizza nel commettere i crimini di natura tecnologica.. Inoltre, di particolare importanza e' anche la collaborazione che le strutture investigative devono avere con le instituzioni di monitoraggio informatico, le societa' informatiche e qualsiasi altra agenzia e/o instituzione volta a garantire una collaborazione in termini di servizi, finalizzate ad una buona riuscita dell'attivita' investigativa.

Allo stato il cybercrime sta maturando la sua esperienza in rete diventando sempre piu' difficile da individuare, identificare e combattere. L'utilizzo dei scudi inforamtici da parte dei hacker, e l'utilizzo di meccanismi di truffe sempre piu' sofisticate, fa si che il criminologo, l'investigatore specializzato ed il supporto normativo sia sempre piu' debole e non al passo con l'evoluzione teconologica del crimine.

Ecco, dunque, che e' indispensabile essere sempre al passo con le nuove teconologie, analizzare, studiare e, a volte, incimentarsi in raggionamenti da cybercriminali, per poter, cosi' raggiungere il risultato e combattere questi nuovi fenomeni criminali.

1. Cybercrime - cybercriminal: Riflessioni terminologiche

Il *Cybercrime* è qualsiasi attività criminale che coinvolge i computer, Internet, la rete fissa e qualsiasi altra rete di comunicazione che serve a scambiare informazioni e metterle in rete.

La figura del *cybercriminale* mira a danneggiare o distruggere i sistemi informatici al fine di ottenere informazioni in maniera illecita o danneggiarli, nonché egli mira alla diffusione in rete della propria attività criminale, quale la diffusione di immagini che ne possano violare l'integrità e la dignità della persona, la distribuzione di materiale di natura penale, cioè di tutta quella attività prevista dal Codice penale come reato o comunque, condotta meritevole di punizione.

L'attività più comune dei criminali informatici, spesso soprannominati "hacker", è quella di catturare informazioni relative all'ambito finanziario, con l'obiettivo di utilizzare tali informazioni per ricattare i legittimi titolari delle stesse.

Sia negli Stati Uniti d'America che nell'Unione Europea, l'attenzione delle autorità di vigilanza in materia di cybersecurity è focalizzata proprio sulla prevenzione e il perseguimento dei reati finalizzati all'acquisizione illegittima di dati, alla distruzione delle reti di comunicazione, alla danneggiamento dei sistemi informatici, con conseguenze economiche per i fornitori di servizi, violazione del diritto d'autore o violazione dello stesso, molestie sessuali attraverso l'uso di piattaforme online, cyberbullismo, ecc.

Il Cybercrime può essere utilizzato anche dalle organizzazioni criminali a fini di traffico di stupefacenti, traffico attraverso la rete di beni custoditi da "marchi registrati", produzione, detenzione o distribuzione di materiale pedopornografico che coinvolga minori, ecc. Lo svolgimento di tali attività in rete – internet -, ha fatto sì che questa tipologia di reati assumono una forma transfrontaliera indefinita, che non necessita più della presenza fisica dei suoi autori nel realizzare l'attività delittuosa.

Principalmente, i crimini informatici in campo economico restano con il più alto margine d'azione, in particolare la violazione dei codici di accesso all'e-banking, la manipolazione di attività nel campo del commercio elettronico, la truffa online e la falsificazione di dati personali al fine di utilizzarli per altre attività che si svolgono in un determinato territorio, come ad esempio, il furto dei dati personali per creare e clonare carte di credito utilizzabili da "hacker" in diverse banche.

Il Cybercrime può essere commesso sia da un singolo individuo che da un gruppo di persone, è sufficiente che questi possiedano competenze informatiche in grado di ottenere illegittimamente informazioni, violare i sistemi di sicurezza e ricavare altri dati importanti per la prosecuzione dell'iter criminale che intendono realizzare.

Un altro elemento essenziale del profilo criminale dei criminali informatici è il fatto che scelgono di operare in luoghi in cui il livello di sicurezza informatica, le leggi penali in ambito cibernetico sono deboli o inesistenti[1].

Ciò ha reso la loro attività difficile da condannare, poiché la normativa punitiva del Paese in quest'area rimane bassa o inesistente.

1 Marchetti R – Mulas R., Cybersecurity: Hacker, terroristi, spie, e le nuove minacce del web, Luiss Press, Roma, 2017, fq. 42.

1.1 *Come si realizza il cybercrime*[2]*?!*

Il *cybercrime* evolve insieme alle altre forme di comunicazione. Così, ogni metodo di lavoro in rete diventa oggetto di studio e analisi inversa da parte dei cybercriminali, che ogni volta perfezionano la propria tecnologia cognitiva in relazione ai vari sistemi oggetto del loro attacco.

Alcuni dei metodi più popolari utilizzati dagli "hacker"[3] sono:

- La Distribuzione del sistema DDoS, questo tipo di sistema garantisce agli hacker di spegnere il sistema di comunicazione di rete, ad esempio Intranet, o chiusura della comunicazione sulla rete - Internet, paralizzando l'intero sistema di comunicazione.
- In generale, questo è l'attacco più semplice degli hacker che, dopo questa manovra, spesso cercano di estrarre altre informazioni destabilizzando la vittima e facendo in modo che gli hacker abbiano l'accesso più facile al sistema di comunicazione nel tentativo di riaprire e catturare le informazioni che cercano.
- Infettare i sistemi operativi o le reti con virus, come ad esempio, il più famoso, il Troian. Con il rilascio di virus, gli hacker mirano a infettare il sistema e de crittografare le informazioni, in modo da poter utilizzare, poi, le informazioni ottenute dal sistema o dalla rete attaccata, in modo rapido e senza troppi sforzi. Il rilascio di questi virus è spesso creato appositamente per il sistema che viene attaccato.
- Il phishing è un altro noto fenomeno di hacking in rete, principalmente su piattaforme online, dove il metodo utilizzato è quello di inviare e-mail false, appositamente studiate per catturare informazioni, distruggendo il sistema di lavoro. In particolare, questo metodo viene utilizzato per le aziende dotate di un sistema di comunicazione elettronica, interno, intranet o esterno, tramite l'invio di link o e-mail che va violato.
- Gli attacchi di identificazione sono volti al furto di dati personali di soggetti, siano essi persone fisiche o giuridiche che utilizzano in rete proprie informazioni sensibili, come ad esempio hanno accesso a siti di e-banking da cui effettuano transazioni economiche, hanno accesso a siti di e-commerce dove effettuano transazioni commerciali,

2 Intervento presentato dall'Avv. Ph.D. Enida Bozheku, al II - Convegno Nazionale "*Ordine, Sicurezza e Comunità*", Facoltà di Scienze Umane, Università "Ismail Qemali", Valona, maggio 2019.

3 https://searchsecurity.techtarget.com/definition/cybercrime, accesso il 12.07.2022.

ecc.. L'attacco viene effettuato principalmente installando, o chiavi crittografate tramite software o, analizzando i punti deboli del software utilizzato dalla vittima e, quindi, attaccando direttamente il luogo di archiviazione delle informazioni.

- Un'altra attività criminosa svolta tramite gli attacchi informatici è quella di interferire con banche dati online, come ad esempio dati che operano nella rete del fisco, università, banche, polizia di stato, ecc.. Interferendo nei sistemi di questi enti, gli hacker sono in grado di modificare i dati, eliminarli o rubarli per rivenderli a terzi sotto forma di ricatto o guadagno di altro. Pertanto, per strutture di questo livello, la protezione informatica richiede un elevatissimo livello di professionalità nel campo dell'informatica e dei programmi utilizzati per la protezione dai cyber - attacchi.
- Un altro profilo penale legato agli attacchi informatici è quello relativo all'ottenimento di dati direttamente riconducibili a società commerciali, principalmente quelle che forniscono servizi nel campo della brevettazione della proprietà intellettuale, servizi bancari in qualità di intermediario (es. Paypal), altri dati di informazioni sensibili tutelate dalla legge, eccetera.
- Altro aspetto penale, che coinvolge la rete, è quello della commissione di reati di natura personale, che si realizzano attraverso profili "account" aperti su vari siti web o social media o piattaforme social, con l'obiettivo di "colpire" la vittima, che può essere minorenne, nonché il mettere in atto molestie sessuali verso un adulto, diffamazione, insulti o bullismo online di minori da parte di altri minori utilizzando le piattaforme online oppure l'utilizzo di profili falsi per presentare schemi di frode che vengono eseguiti interamente online, ecc..

2. Digital Profiling: elemente karakterizuese

Con l'avanzare della tecnologia, anche l'attività investigativa da parte degli organi competenti ha cambiato approccio e ora richiede un livello di specializzazione più elevato.

Le nuove tipologie criminali, ora, vengono interamente commesse in rete, facendo che anche gli investigatori "scendano" in rete al fine di rintracciare e poi punire i soggetti agenti in questa nuova scenza del crimine.

Il Cybercrime viene realizzato attraverso l'utilizzo di un computer, il

quale essendo comandato dalla mente umana, ha un ruolo fondamentale nel realizzare l'attività criminale. Tramite il computer, il crimine può venire commesso sia in forma attiva, quindi il computer fa da mezzo per compiere il crimine, sia in forma passiva in cui il computer è l'oggetto stesso del crimine in quanto, in esso sono contenuti i dati delittuosi (e.s. la detenzione di materiale pedopornografico di minori ai fini della vendita del materiale online).

In questo contesto, Il *Digital Profiling* si inserisce, quindi, come metodologia per l'isolamento e l'analisi delle caratteristiche umane all'interno di una serie di crimini informatici. Esso comprende una serie di metodologie per tracciare profili psicologici, anagrafici e comportamentali degli autori di reato, partendo agli elementi emersi nelle indagini preliminari, per poi proseguire nell'analisi vittimo-logica, scena del crimine e delle procedure di *computer forensics*.

Da un punto di vista schematico, il *digital profiling*[4] consiste in:

Profiling elements	Decision Models – Apply sistem	Crime Assessmant	Criminal Profiling
Acquisizione dati delle strutture e delle figure coinvolte, architettura dei sistemi, procedure di *incident responseed* acquisizione in *computer forensics,* raccolta dei dettagli fisici e delle prove	Raccolta e inserimento dati e file di log in software di analisi e database, elaborazione dati, suddivisione in categorie, creazione di un modello di dati appropriato alle caratteristiche informatiche dell'indagine	Valutazione delle caratteristiche informatiche dei sistemi coinvolti, delle metodologie e degli strumenti utilizzati per il crimine ed impatto conseguente. Analisi di eventuali collegamenti e caratteristiche socio/politiche. Estrazione dati comportamentali significativi.	*Link analysis, Data Mining*, elaborazione del profilo informatico e dei collegamenti psicologici.

4 https://www.igorvitale.org/tecniche-digital-profiling-supporto-investigazioni/, accesso il 10.07.2022.

2.1 Il Computer forensics

Nel costruire tutta la struttura inerenti alle figure professionali volte a tracciare i crimini informatici, non può mancare il computer forensics.

Questa è una branca della cybersecurity, la quale insieme al *digital profiling*, utilizza tecniche investigative per identificare e archiviare prove da un dispositivo informatico ad un altro. I dati raccolti dal computer forensics vengono utilizzati come prove nei vari procedimenti penali e non solo, ma anche a quelli di natura civilistica e/o amministrativa. A volte i professionisti in questo campo potrebbero essere chiamati a recuperare i dati persi da unità guaste, server che hanno subito un arresto anomalo o sistemi operativi che sono stati riformattati ecc..

L'informatica forense rappresenta, oggi, un aiuto essenziale nelle indagini, in quanto, molte volte, in materia di indagini investigative, uno dei luoghi più comuni in cui cercare indizi è il computer o il cellulare di un sospettato. Ed è, proprio qui, che entra in gioco un professionista dell'informatica forense. Dunque, nell'ambito informatico il supporto tecnico specializzato di computer forensics, è di fondamentale aiuto per gli investigatori, i quali grazie alla raccolta dati di natura informatica che vengono assunti dagli informatici forensi possono costruire l'iter criminale ed il relativo modus operandi per giungere, poi, al fermo del soggetto sospettato.

Attualmente, il computer forensics non ha una determinazione giuridica specifica, ma nella prassi essa viene definita come[5]: "*Il computer forensics è quella disciplina, di matrice tecnologica che unisce elementi di diritto e informatica per raccogliere e analizzare dati da sistemi informatici, reti, comunicazioni wireless e dispositivi di archiviazione di modo che sia ammissibile come prova in un tribunale*".

3. Alcune tipologie di reati consumati in rete

Parlando di cybercrime, gli addetti ai lavori hanno suddiviso l'area in due macro-schemi:

a) Crimini diretti ad attaccare le reti informatiche ed i computer ad essi connessi;

b) Crimini facilitati dalle reti informatiche e dai computer connessi

❍ a1) Nel primo gruppo fanno parte tutti quei reati, i quali hanno quale

5 https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf, accesso il 2.07.2022.

finalità la violazione dei sistemi informatici al fine di ottenere un profitto per sé o per altri, per conto dei quali agiscono. Il fine ultimo di questi cybercriminali è il corrispettivo in danaro del loro agire criminale (p.e.s.: furto di identità, sottrazione di dati coperti da segreto (dati bancari), phishing ecc..). Il soggetto agente viene definito hacker.

- b1) Nel secondo gruppo fanno parte tutta quella gamma di reati, i quali possono essere realizzati anche senza l'utilizzo dei mezzi informatici e computer ad essi connessi, ma che, i criminali per poter agire in maniera più spedita e senza inibizioni, utilizzano la rete, la quale, di fatto, favoreggia il loro agire criminale.

3.1 *Gli Hackers*

Gli Hackers sono individui i quali hanno capacità specifiche per quanto attiene il mondo dell'informatica. Essi sono esperti di programmazione, linguaggi e sistemi operativi tecnologici, in grado di penetrare e scoprire i punti deboli dei sistemi di sicurezza.

Gli hackers hanno doti naturali in campo tecnologico, le quali le utilizzano per accedere in maniera furtiva a vari sistemi operativi e, di conseguenza, generare in questi sistemi problemi di vario tipo.

Gli hackers[6] essendo esperti informatici, utilizzano la tecnologia per procurare vantaggio a sé o ad altri, nel caso in cui i loro servizi venissero richiesti da terzi. Di solito l'hacker realizza attività criminali punite dalla legge dello stato ai danni del quale agisce.

Gli Hacker [7]vengono suddivisi in tre categorie:

a) **Crackers**: sono coloro che penetrano nei sistemi informatici più complessi ed a più livelli di protezione. Sono di solito soggetti con capacità informatiche fuori dal comune che agiscono per infettare il sistema operativo in cui accedono o sottraggono i dati per ottenere un proprio vantaggio economico.

b) **Hackers**: soggetti che penetrano nei sistemi informatici con un buon livello di sicurezza ma non infallibile ed impenetrabile. Sono esperti

6 Petherick, W. A., & Turvey, B. E., *Criminal Profiling: Science, Logic, and Cognition*, Elsevier, In Criminal Profiling, 2012, pgg. 41-65.

7 Enrici I., Ancilli M., Lioy A., (210), A Psychological Approach to Information Technology Security file:///C:/Users/user/Downloads/Enricietal2010HSI2010Proceedings%20(2).pdf, accesso il 30.06.2022.

nell'individuare le falle del sistema ed attaccare.

c) **Rodents:** soggetti con capacità informatiche di base, di solito self-made, e che la loro maestria si manifesta per lo più nel sottrare password e dati di carattere privato, quale I.D. o numeri di carte di credito immesse online in siti di e-commerce.

In merito al profilo psicologico degli Hacker, ossia le motivazioni che spingono un hacker ad agire, la dottrina[8] ha individuato 5 tipologie:

1. **Hackers occasionali**: soggetti che di solito mettono alla prova le proprie capacità in campo informatico, come spinta emotiva piuttosto che intellettiva
2. **Hackers politici** (spinti da motivi politici, di natura emotiva, in cui vogliono dimostrare i propri valori e credo politico)
3. **Crimine Organizzato** che utilizza gli hackers come propri membri e/o soggetti loro collaboratori per ottenere vantaggi economici
4. **Squatters**: hanno quale motivo quello di accedere a database con informazioni rilevanti e di natura sensibile per poi vendere i dati al miglior offerente.
5. **Insiders**: soggetti i quali lavorano per l'azienda e dall'interno agiscono sul sistema informatico.

   5/1 **Intruders**: soggetti i quali si introducono illegittimamente nell'azienda per estrarre informazioni dai computer della stessa.

3.2. *I Cybercrime di matrice sessuale*

Come già accennato i crimini informatici sono di varia natura e specie. Attualmente la gamma dei reati che si compiono a mezzo internet e computer connessi è aumentata a dismisura, dove molti reati di natura personale stanno avendo un incremento non indifferente. E proprio in questo senso che la dottrina sta articolando nozioni quali:

- Cybestalking
- Cyberbylling
- Pedo-pornografia online

8 Lafrance Y., (2004) Psychology: A precious security tool. http://www.sans.org., accesso il 30.06.2022.

- Grooming[9]
- Revenge Porn
- Sextortion

La tecnologia se per un lato sta aiutando e migliorando la vita delle persone, dall'altra parte essa diventa sempre più pericolosa per quanto riguarda l'utilizzo da persone sia mentalmente instabili, sadiche, con tendenze criminali, pedofili, molestatori e violentatori seriali.

In questo senso, il libero accesso ad internet e la celerità dell'assunzione delle informazioni fa si che i soggetti a tendenza criminale possano utilizzare internet, in maniera assai semplice per rintracciare le proprie vittime e, di conseguenza mettere in atto il proprio scenario criminale.

Così, uno dei reati che si sta scontrando di più nella pratica investigativa sono quelli a sfondo sessuale.

Infatti, grazie a media sociali quale Facebook, Instagram ed altre reti di contatto tra le persone, i predatori sessuali, possono trovare in maniera assai facilitata la propria vittima.

1. **Cyberstalking,** è la sindrome del soggetto molestatore affetto da una dipendenza patologica con la propria vittima.

Infatti, lo stalker nella vita reale è un ex-fidanzato, marito, moglie o semplice corteggiatore, il quale, pone in essere comportamenti che violano la tranquillità e la serenità del soggetto vittima. Il stalker utilizza uno schema prevaricante, invasivo, che consiste nel porre in essere atti ripetitivi quali pedinamento, innumerevoli telefonate, lascia messaggi telefonici, si fa trovare nei luoghi frequentati dalla propria vittima, fa appostamenti.

La tecnologia in questo senso ha fatto si che lo stalker, oltre ad utilizzare i classici metodi, di parvenza fisica, con l'aiuto di internet può attuare altre attività di prevaricazione e molestia quali: l'utilizzo di dispositivi di comunicazione elettronica (e-mail), l'utilizzo di profili falsi di Facebook, l'utilizzo di altri mezzi di comunicazione collegati alla rete internet quali whats up, viber, telegram, Instagram ed altro mezzo di contatto, facilitato dall'utilizzo della rete.

9 Nicola, H., & Powell, A., *Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law,* Social & legal studies, 2016, 25(4), 397-418. - https://journals.sagepub.com/doi/10.1177/0964663915624273.

In questo senso, oggi, si parla di cyber-stalking, dove il soggetto agente ha a propria disposizione la tecnologia per molestare, infastidire e perseguitare la propria vittima.

Nel codice penale albanese, il cyberstalking, non è previsto come tipologia assestante, e quindi la dinamica dell'agire dello stalker si deve ricercare nel modus operandi dell'agente. La norma incriminatrice, allo stato, è sprovvista di una determinazione specifica di legge, nella quale l'utilizzo della rete possa essere configurata come una circostanza aggravante a sé, o anche come forma tipica del reato. In questo senso, per poter parlare di cyberstalking nel Codice penale albanese, esso va riferito esclusivamente al "metodo" in cui opera il soggetto. Infatti, all'art. 121/a del Codice Penale albanese si legge: "*La minaccia o la molestia della persona a mezzo di condotte reiterate, in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita, è punito con la reclusione da sei mesi a quattro anni*".

Come si evince dalla norma, essa non specifica in maniera chiara e precisa, il fatto che il reato di stalking può essere commesso anche a mezzo internet, ma dal tenore della stessa, nella locuzione "*a mezzo di condotte reiterate*", proprio nella parola "***condotte***", è desumibile il fatto che, lo stalking può realizzarsi anche a mezzo internet.

Le caratteristiche di uno **cyberstalker**[10] sono:

- Invio di e-mail in continuazione dal tenore offensivo, minaccioso e prevaricatore;
- Chiamate sul cellulare, messaggi su piattaforme online collegate in numeri non indifferenti e con cadenza temporale precisa (ogni ora, ogni 2 ore e cosi via);
- Diffamazione su piattaforme online pur di discreditare la propria vittima;
- Accesso intrusivo a profili ed account della propria vittima
- Commenti assidui su ogni commento effettuato dalla propria vittima, senza un apparente colleganza.
- Chiamate da terzi, commissionate dallo Stalker ai fini di creare

10 https://www.disputer.unich.it/sites/st13/files/vecchie_e_nuove_dipendenze_2016-2017_prof._sivilli_cybercrime.pdf, accesso il 26.06.2022.

situazioni di disagio nella propria vittima (e.s. finte telefonate da soggetti che sono state pagate dallo stalker per fare finta di essere il fisco, la polizia, l'ospedale ecc..)

2. **Cyberbullying:** E' la modalità, online, tramite la quale un minore pone atti persecutori, molesta e invade la vita di un altro minore. Di solito il bullismo trova campo di applicazione nella vita quotidiana dei giovani, ancora minori, ove coetanei utilizzano sia la violenza fisica che quella mentale per perseguitare la propria vita. Il cyberbullismo si svolte nella piattaforma online, a mezzo di pettegolezzi che vengono divisi sui cellullari dei compagni di scuola, o cerchia di amici, mail e social network.

Il fine del cyberbullo è quello di arrecare uno stato emotivo sottomesso del minore e distruggere la sua autostima. Tali atti prevaricatori vengono messi in atto, inscenando situazioni di particolare impatto psico-fisico per il minore, insultandolo, mettendolo in imbarazzo dinanzi agli altri, con solo fine di distruggere la reputazione del minore. In concreto, attualmente, il codice penale albanese, riconosce solo lo stalking, e non prevede una norma penale spcifica per il cyberbullying. Di guisa che, come asserito nel brocardo latino "*nullum crime sine legge*", nessuno può essere punito per un fatto non previsto dalla legge come reato. Il cyberbullo di solito è un minore conosciuto dalla propria vittima, ma che in rete per porre in essere il proprio piano denigratorio si nasconde dietro l'anonimato. L'attacco cyber del bullo ha, potenzialmente, un infinità di spettatori e produce la moltiplicazione degli stessi, in quanto l'accesso alla rete è di fatto, illimitato.

3. **La pedopornografia online:** E' un problema che assale la società in maniera costante. I pedofili sono sempre in agguato ed hanno un profilo criminale assai chiuso è difficile da rintracciare. In questo senso, la tecnologia, ha fatto sì che questi soggetti potenziassero il loro agire in rete e di conseguenza la loro presenza nel cyberspace sta diventando sempre più incisiva e difficile da controllare.

La pedopornografia online è la produzione, diffusione e commercio su internet di materiale pedo-pornografico. Le funzioni della pedopornografia sono collegate gli istinti di gratificazione sessuale del soggetto agente, all'adescamento del minore ed al profitto.

Il pedofilo raccogli e custodisce materiale pornografico di minori al fine

di utilizzarli per sé o per venderli e/o scambiarlo con altri pedofili. Infatti, il materiale consiste in raccolta di video, immagini, fotografie, web cam, i quali, in seguito, vengono scambiati o pubblicati in appositi siti internet, operanti nel settore della pornografia minorile.

- Nel codice penale albanese, allo stato non esiste una norma specifica a difesa dei minori in ambito di pedopornografia online, l'unico appiglio giuridico desumibile viene estratto dal dettato normativo dell'art. 117, comma 1, cpv c.p.a. "*La produzione, la diffusione, la pubblicità, l'offerta, la messa a disposizione, la trasmissione, l'utilizzo oppure il possesso di pornografia minorile, nonché la creazione di un accesso in maniera consapevole in esso, con ogni mezzo e forma, è punito con la pena di anni tre fino ad anni dieci di reclusione*".

Come si legge dalla norma il riferimento al cyber è inesistente, esso può evincersi solo dal riferimento testuale di "possesso di pornografia minorile", ove si può intendere il possesso del materiale al computer o in file specifici su internet quale "l'i cloud" oppure, il riferimento "***all'accesso con ogni mezzo e forma***", si riferisce anche agli accessi su siti online, in quai vengono trattati materiali di pornografia minorile. In una chiara mancanza previsione di legge, il fatto della consumazione del reato online rimane a stretta discrezione interpretativa della norma penale da parte del magistrato addetto ai lavori,

4. **Il Grooming:** E' una tecnica di adescamento dei minori in rete da parte dei pedofili. Questo termine viene utilizzato per segnalare la modalità di adescamento del minor, la quale forma è quella dell'utilizzo della rete. Le forme di adescamento in rete possono variare da persona a persona ma, volendo generalizzare, il metodo è quello attraverso l'utilizzo delle chat, sms, e-mail, whats up, Facebook, Instagram, e la rete internet in generale.

Il grooming[11] dà la possibilità al pedofilo di scegliere la propria vittima basandosi sulle informazioni che ella ha condiviso in rete. Inoltre, per il pedofilo entrare in una conservazione con il minore diventa più facile se egli si traveste "virtualmente" da un coetaneo del minore stesso. In questo modo creando profili falsi, con caratteristiche simili alla vittima – minore, il pedofilo sarà più ben accettato per conoscersi da minore preda.

Il pedofilo che utilizza la rete per adescare minori, ha un profilo personale di natura chiusa, introverte, generalmente di buone maniere e proveniente da

11 Bowker A., *Investigating Internet Crimes*, Elsevier, Waltham, Ma, 2014, pg. 33.

una situazione sociale di comodo.

All'interno del sistema, la dottrina ha identificato tre categorie di cyberpedofili:

a) **Dabbler**: pedofili, di natura curiosa che utilizzano per lo più la pedopornografia (immagini, video ecc.).

b) **Preferential**: pedofili, ma che nella loro vita quotidiana possono avere relazioni sessuali anche con adulti del proprio o dell'altro sesso.

c) **Club**: Pedofili, che utilizzano la rete, per condividere con altri pedofili sia materiale pedopornografico che le proprie esperienze e per assumere informazioni su eventuali minori "disponibili" e "raggirabili".

Attualmente, nel Codice Penale albanese, la categoria dei **grooming** non è prevista è non esiste una norma penale specifica a tutela del minore in caso di adescamento su rete da parte di un pedofilo.

5. **Revange Porn[12]:** E' una forma di vendetta attuata online da un ex fidanzato, moglie, marito o compagno, o comunque da un soggetto con il quale si sono intrattenuti rapporti di natura sessuale. In questa tipologia di crimine, il soggetto agente per vendicarsi del soggetto che ha avuto rapporti intimi, pubblica su internet video e/o immagini di natura sessuale volti a danneggiare la reputazione della vittima. Questo reato si consuma, sulla rete, in quanto il video e/o l'immagine, una volta messa in rete è particolarmente difficile da cancellare. Attualmente, nel Codice penale albanese non c'è una norma a tutela di questa tipologia di condotta posta in essere ai danni di un'altra persona. L'unico riferimento normativo invocabile e la violazione della privacy, la quale viene considerato reato ai sensi dell'art. 121 del codice penale "*L'intromissione illegittima nella vita privata altrui*", ove però manca specificatamente la previsione del fatto incriminato ossia la pubblicazione di video di natura sessuale ai fini di vendetta personale.

6. **Estorsione Sessuale13 Online:** E' una condotta di natura criminale volta ad ottenere danaro e/o altri favori dal soggetto con il quale

12 Greco F., Greco G., (2020), *Investigative techniques in the digital age: Cybercrime and Criminal Profiling*, European Journal of Social Sciences Studies, online, ISSN, 2501-8590 - file:///C:/Users/user/Downloads/INVESTIGATIVE_TECHNIQUES_IN_THE_DIGITAL_AGE_CYBERC.pdf.

13 Ziccardi G., Perri P., *Tecnologia e Diritto*, Giuffrè, Milano, 2014, pg. 33.

si è intrattenuto o si intrattiene un rapporto intimo. Il soggetto agente ricatta l'atra persona che se non acconsentirà a fare e dare ciò che gli si ordina, verrà pubblicato su Internet il video o i video e/o altre immagini che ritraggono la persona in atteggiamenti a sfondo sessuale.

Per ottenere i video e le immagini intimi, il soggetto agente deve avere avuto comunque un coinvolgimento da parte dell'atra persona a porre in essere attività sessuali virtuali, di solito consistenti in auto-erotismo. Attività questa che all'insaputa ma anche, eventualmente, con il consenso dell'altra persona vengono registrate.

Anche questa tipologia di cybercrime non è prevista dal codice penale albanese. L'unico riferimento è desumibile dell'art. 121 del codice penale "*L'intromissione illegittima nella vita privata altrui*", che, in realtà non corrisponde alla condotta posta in essere.

4. Il profilo psicologico del cybercrime

In precedenza, abbiamo visto varie tipologie di condotte delittuose le quali si possono commettere utilizzando la rete ed il computer ad essa connesso.

In questo senso anche da un punto di vista criminologico, il soggetto agente nel mondo del cybercrime presenta delle caratteristiche specifiche, a volte molto diverse dal comune criminale.

Infatti, nel cybercrime si nota che il soggetto agente[14] ha una percezione del crimine ben diversa da come la vivrebbe nella realtà. Infatti, molto spesso egli utilizza Internet, ma in alcune situazioni non sa nemmeno che sta compiendo reato, in quanto la percezione della condotta illegittima è meno sentita. In questo senso anche la percezione che alla vittima si stia facendo realmente del male non viene percepita come reale e come situazione passibile di punizione. Il fatto che il computer si interpone tra il soggetto agente e la vittima fa si che anche la gravità della condotta criminale venga meno.

Nel cyberspazio, ci agisce al fine di attuare attività considerate se non penalmente rilevanti almeno umanamente tali, si sente libero e fuori da ogni restrizione giuridica. In questo senso, il pedofilo che agisce nel cyberspazio non oserebbe attuare attività di grooming se non ci fosse il computer, stesso valga per un truffatore, il quale utilizza il computer per creare uno schema

14 Douglas, J. E., Ressler, R. K., Burgess, A. W., & Hartman, C. R. *Criminal profiling from crime scene analysis.* Behavioral Sciences & the Law, 1986, 4(4), 401-421, accesso il 4.07.2022.

truffaldino, oppure donne che non avrebbero il coraggio di prostituirsi per strada ma utilizzando il cyberspazio possono nascondere il proprio volto e porre in essere attività di sesso virtuale senza alcune remore.

Il profilo di questi soggetti risulta caratterizzato da un carattere non violento, attitudine a controllare i propri movimenti e schema di agire, tendenza ad operare in solitudine, minore capacità di auto-concepirsi come criminale, capacità informatiche volte a facilitarli il lavoro per raggiungere il proprio interesse.

5. Conclusioni

Il Cyberspazio, da un punto di vista giuridico, è molto vasto, pieno di insidie e senza una regolamentazione precisa volta a combattere i fenomeni negativi che si presentano di volta in volta.

L'evoluzione rapida della tecnologia sta trasformando anche il modus operandi dei criminali, i quali, sempre e di più, stanno sfruttando gli sbocchi informatici al fine di perfezionare il proprio agire delittuoso. Il computer forensics, il digital profiling, e più in generale il cybercrime, si stanno sviluppando rapidamente, spostando l'arena investigativa e criminale dal reale al virtuale.

In quest'ottica sembra, però, che le legislazioni degli stati non siano adeguatamente conformate a questa evoluzione del crimine, e pertanto, sembra indispensabile che, alla luce di questo cambiamento, anche le legislazioni si adeguino.

In questo lavoro, è stato preso ad 'esame il Codice penale albanese, riferendole ad alcune tipologie di nuove condotte criminali che si stanno, attualmente, manifestando in rete ma la risposta del legislatore è insufficiente in quanto mancano le norme penali specifiche, volte ad inquadrare tali fattispecie giuridiche. E se la legge manca, il crimine non esiste.

Tenendo a mente questi sviluppi sembra d'obbligo che il Codice penale albanese venga ristrutturato, ed al suo interno venga creata un'area specifica ove inquadrare i crimini informatici, di modo che, anche reati quali il revenge porn, l'estorsione sessuale online, il grooming ed altre tipologie di reati informatici possano essere puniti in maniera adeguata, proporzionale ed in conformità alle conseguenze da essi prodotte.

Bibliografia

Bowker A., *Investigating Internet Crimes*, Elsevier, Waltham, Ma, 2014, pg. 33

Codice Penale Albanese

Douglas, J. E., Ressler, R. K., Burgess, A. W., & Hartman, C. R. Criminal profiling from crime scene analysis. Behavioral Sciences & the Law, 1986, 4(4), 401-421.

Intervento presentato dall'Avv. Ph.D. Enida Bozheku, al II - Convegno Nazionale "*Ordine, Sicurezza e Comunità*", Facoltà di Scienze Umane, Università "Ismail Qemali", Valona, maggio 2019

Marchetti R – Mulas R., Cybersecurity: Hacker, terroristi, spie, e le nuove minacce del web, Luiss Press, Roma, 2017, fq. 42 e vazhdim

Petherick, W. A., & Turvey, B. E., *Criminal Profiling: Science, Logic, and Cognition*, Elsevier, In Criminal Profiling, 2012, pgg. 41-65.

Ziccardi G., Perri P., *Tecnologia e Diritto*, Giuffrè, Milano, 2014, pg. 33

Sitografia

file:///C:/Users/user/Downloads/Enricietal2010HSI2010Proceedings%20(2).pdf

file:///C:/Users/user/Downloads/INVESTIGATIVE_TECHNIQUES_IN_THE_DIGITAL_AGE_CYBERC.pdf

http://www.sans.org. -

https://journals.sagepub.com/doi/10.1177/0964663915624273

https://searchsecurity.techtarget.com/definition/cybercrime, accesso il 12.07.2022

https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf

https://www.disputer.unich.it/sites/st13/files/vecchie_e_nuove_dipendenze_2016-2017_prof._sivilli_cybercrime.pdf, accesso il 26.06.2022

https://www.igorvitale.org/tecniche-digital-profiling-supporto-investigazioni/

ROLI DHE NDIKIMI I TEKNOLOGJISË NË ZHVILLIMIN E SË DREJTËS PENALE DHE PROCEDURËS PENALE

OLGERT RUMNICI
Prokuror në Prokurorinë pranë Gjykatës së Shkallës së Parë Krujë;
olgertrumnici@hotmail.com

PROF. ASOC. DR SKERDIAN KURTI
Dep. i së Drejtës Penale / Fakulteti i Drejtësisë, Universiteti i Tiranës
skerdian.kurti@fdut.edu.al

Abstrakt

Në këtë punim do të paraqesim ato zhvillime ligjore në Kodin Penal dhe Kodin e Procedurës Penale, të cilat janë rezultat i zhvillimeve teknologjike apo i ndikimit të teknologjisë. Gjithashtu, do të përpiqemi të evidentojmë rolin e saj në ndihmë të zbatimit të Kodit Penal përmes përmirësimit dhe drejtimit të hetimit në nivel më cilësor, veçanërisht sa i përket temës së provave në procesin penal. Për këtë arsye, kemi gjykuar të rëndësishme, që zhvillimin e së drejtës penale në raport me zhvillimin teknologjik ta pasqyrojmë përmbledhtazi në mënyrë kronologjike prej momentit të miratimit të Kodit aktual Penal deri në zhvillimet aktule legjislative. Në vijim, do të fokusohemi në raportin e zhvillimeve teknologjike në aspektet procedurale penale, veçanërisht trajtimi i përmbledhur i disa lloje provash, rëndësia dhe efektiviteti i të cilave qëndron pikërisht në përparimin e teknologjisë në fushat përkatëse, ku patjetër me interes janë ekspertimet shkencore

Fjalë kyçe: *zhvillimi teknologjik, kodi penal, kodi i procedurës penale, vepra penale, procesi penale, prova*

1. Hyrje

Shoqëria bashkëkohore dominohet nga teknologjitë e reja, të cilat karakterizohen nga një zhvillim shumë i shpejtë dhe një aftësi tepër të madhe për t'u përhapur në të gjitha fushat e jetës individuale dhe kolektive. Raporti i shoqërisë në tërësi me teknologjinë është një raport i veçantë, vështirë i përshkrueshëm në pak rreshta e kësisoj i nevojshëm studimi i këtij binomi në mënyrë të thelluar dhe multidisiplinare. Ajo që mund të themi me siguri është që kemi të bëjmë me një raport dinamik, të ndryshueshëm në kohë dhe hapësirë.

Sipas mendimit tonë, në një masë të madhe njerëzish, që imagjinojmë se janë shumicë, ekziston mendimi i përgjithshëm se zhvillimi i teknologjisë ka ndikuar në përmirësimin e shoqërisë dhe jetës në tërësi. Priremi të përkrahim aforizmin se nuk ka teknologji të keqe apo të mirë, por mënyra se si ne njerëzit e përdorim mund të jetë e mirë apo e keqe; të paktën deri në momentin kur teknologjia mund të përdorë njeriun. Me pak diferenca, në gjykimin tonë ndoshta të pandjeshëm, mund të thuhet me siguri se përgjithësisht teknologjia dhe shoqëria janë zhvilluar reciprokisht dhe paralelisht. Themi përgjithësisht, pasi kjo mund të jetë e vërtetë për disa struktura apo entitete që përbëjnë shoqërinë njerëzore si ekonomia, kultura, arsimi, mjekësia, por nuk mund të thuhet e njëjta gjë per drejtësinë. Kjo e fundit duket se deri në zhvillimet e shek.XX ka qenë e pandjeshme në raport me zhvillimet teknologjike ose ato kanë qenë një hap përpara zhvillimit të drejtësisë. Edhe në fushën e procedimit penal, përdorimi i mjeteve të avancuara teknologjike ka ndryshuar ndjeshëm fizionominë e sistemit, me ndikim të dukshëm në praktikat[1], por edhe në të drejtat[2], garancitë dhe institucionet kyçe. Duke dashur të ofrojmë të paktën një pasqyrë të përgjithshme të aspekteve të sistemit më të prekura nga ndikimi i evolucionit teknologjik në procesin penal, mund të vëmë re se pothuajse çdo sektor i tij është ndikuar, edhe pse në mënyra të ndryshme dhe me intensitet më të madh ose më të vogël në varësi të rasteve. Fusha e provave penale është ajo që vjen menjëherë në mendje, pasi është i ashtuquajturi sektori i provave dixhitale dhe të automatizuara që është bërë gjithnjë e më i rëndësishëm në praktikën e përditshme të drejtësisë penale:

---

1 Një mendim që mund të shtrohet për diskutim lidhet me zhvillimin e procesit penal në kohë pandemie, referuar edhe pandimisë së shkaktuar nga covid 19 dhe përdorimit të teknologjisë. Shih, G. Spangher, *Covid-19: nel disastro si vede chiaro*, në Penale Diritto e Procedura, Rivista trimestrale, Nr.1/2020.

2 Shih, G. Ubertis, *Giustizia penale e nuove tecnologie*, në Diritto Penale Contemporaneo, Rivista Trimestrale, Nr.4/2020. Theksohet kujdesi që udhet të tregojmë gjatë përdorimit të teknologjisë dhe veçanërisht në fushën e ruajtjes së privatësisë apo edhe të jetës familjare të mbrojtura edhe nga neni 8 i Konventës Evropiane për të Drejtat e Njeriut.

mendoni për kërkimet dhe sekuestrimin e dokumenteve elektronike, marrjen procedurale të e-maileve ose sms-ve, deri në kapjet e kryera drejtpërdrejt nëpërmjet viruseve kompjuterike të instaluara në pajisjet e personit të përgjuar. Nuk ka dyshim se teknologjia mund t'i ofrojë sistemit të drejtësisë penale mjete të dobishme në nivele të ndryshme[3]. Procesi penal i një vendi të caktuar është pasqyrë e shoqërisë që jeton në atë vend, kështu që nëse sot, ky proces bazohet në një arsenal teknologjik në zgjerim dhe evolucion të vazhdueshëm, është e pamundur që zhvillimi i procesit të mos e marrë parasysh zhvillimin teknologjik, dhe nga ana tjetër duhet të pranojmë se mjetet më të sofistikuara teknologjike ofrojnë një gamë të gjerë përfitimesh të mundshme për të gjithë sistemin. Është konstatim i saktë dhe i vërtetë që në shumicën e rasteve drejtësia vepron kryesisht në retroaktivitet, pra, ajo përpiqet të rregullojë situata të cilat kanë ndodhur më herët ose të veprojë edhe në proaktivitet duke përdorur të mira teknologjike të krijuara gjithsesi më herët. Sigurisht, nuk mendojmë se ka qenë gjithnjë kështu, e këtu sjellim në vëmendje disa periudha kulminante të zhvillimit të drejtësisë; e drejta romake, e drejta e sheriatit, e drejta kanonike, *common law* etj. Prej shekullit XX dhe aktualisht çështja që vlen të diskutohet ka te beje pikërisht me faktin e impaktit te teknologjisë në drejtësi, me fokus të veçantë në drejtësinë penale, aty ku edhe risku i cenimit të të drejtave dhe lirive themelore të individit është më i madh, po të kemi parasysh se objekt i cënimit mund të jetë jeta, shëndeti, liria, pasuria apo edhe privatësia[4]. Në këtë punim do të përpiqemi të evidentojme pikërisht këtë impakt në të drejtën tonë penale dhe procedurë penale, duke e vënë theksin edhe te roli i dyfishtë i teknologjisë si mjet i kryerjes së veprave penale të ndryshme dhe teknologjisë si mjet për parandalimin dhe luftimin e kriminalitetit.

2. Përqasja e Kodit Penal shqiptar me zhvillimet e teknologjisë

Duhet kuptuar që teknologjia po aq sa është e dobishme për të luftuar kriminalitetin e çdo lloj forme, po aq e dëmshme është në duart e gabuara. Anjshtajni, shkencëtari i mirënjohur i shek XX ka thënë se "*Progresi teknologjik është si një sëpatë në duart e një krimineli patologjik*". Në epokën

3 Shih, C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, në Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1167-1188, set.-dez. 2019.

4 Shih, G. M. Baccari, C. Conti, *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, në Diritto Penale e Processo, Mensile di giurisprudenza, legislazione e dottrina, Nr.6/2021.

aktuale, nën efektet e zhvillimit të shpejtë e të shumanshëm teknologjik e shkencor, kjo thënie është vërtetuar, me të gjithë panoramën çfarë ofron realiteti i sotshëm.

Askush disa vite më herët nuk mendonte se terrorizmi[5] dhe krimet e urrejtjes[6], të cilido lloji, do të kryheshin edhe nëpërmjet internetit, nëpërmjet platformave të ndryshme sociale dhe rrjeteve të informacionit masiv. Po ashtu, pak besohej se teknologjia do të përdorej për realizuar veprime të kundërligjshme të vjedhjes së pasurisë, mashtrimit, evazionit me anë të taksave e tatimeve, pastrimit të produkteve të veprave penale. Po aq pak besohej se teknologjia do të përdorej për të nxjerrë apo zbuluar të dhëna me natyrë sensitive publike apo private, apo se kriptomonedhat do të ishin një çështje me interes jo vetëm juridik. Në këtë kuptim, mund të thuhet me siguri se teknologjia, nga pikëpamja objektive e trajtimit të veprave penale të caktuara, përbën mjetin me të cilin mund të kryhet një vepër penale, vendin e kryerjes së saj ose cenimi i saj mund të jetë pasojë e veprës penale.

Nëse i hedhim një vështrim Kodit Penal shqiptar të vitit 1995, në formën e vet fillestare, i pa azhornuar me ndryshimet që janë kryer deri aktualisht, do të vërejmë se në të nuk gjendej asnjë dispozitë që të shprehej në formë tekstuale për teknologjinë si element përbërës i ndonjë vepre penale, si mjet që shërben për realizimin e një vepre penale, si vend i kryerjes së veprës penale apo si pasojë e veprës penale, në kuptimin e cenimit të një rrjeti teknologjik, informatik, database etj. Jo vetëm që teknologjia në atë periudhë ishte në hapat e parë në vendin tonë, por edhe në nivelin në të cilin zhvillohej e përhapej, ligji penal material nuk ishte në gjendje të ofronte mbrojtje juridike të marrëdhënieve të caktuara juridiko-penale që mund të cenoheshin. Mund të gjenden shumë pak vepra penale të parashikuara në Kodin Penal të asaj periudhe, të cilat në mënyrë implicite mund të interpretohen se kanë pasur teknologjinë si rrethanë apo element të veprës penale.Megjithatë, duhet përmendur edhe fakti se në çdo periudhë kohore ka patur një stad të caktuar zhvillimi teknologjik, e cila patjetër është reflektuar edhe në legjislacion[7].

---

5 Shih, R. Pezzuto, *Contenuti terroristici on-line: L'Unione Europea lavora a nuove forme per prevenirne la diffusione*, në Diritto Penale Contemporaneo, Rivista Trimestrale, Nr.4/2019.

6 Shih, V. Nardi, *I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider*, në Diritto Penale Contemporaneo, 2019, https://archiviodpc.dirittopenaleuomo.org/upload/4923-nardi2019a.pdf.

7 Në këtë drejtim mund të permenden si shembuj dispozitat 121 dhe 123 të Kodit Penal. Në nenin 121 të Kodit Penal parashikohej se: "*Vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimi, regjistrimi ose transmetimi i fjalëve, fiksimi, regjistrimi ose transmetimi i figurave, si dhe ruajtja për publikim apo publikimi i këtyre të dhënave që ekspozojnë një aspekt të jetës private të*

Me kalimin e viteve dhe zgjerimin e fushave të aplikimit të teknologjive, u rritën dhe veprimet shoqërisht të rrezikshme, të cilat kryheshin nëpërmjet keqpërdorimit të teknologjisë, por që ende nuk ishin kodifikuar dhe kriminalizuar si vepra penale nga legjislatori. Këtu mund të përmendim mashtrimet financiare të kryera nëpërmjet teknologjisë, falsifikimet, veprat e tjera në fushën e krimeve me natyrë financiare etj.Përpjekja e parë legjislative, në kuadrin e drejtësisë penale, ishte miratimi i ligjit nr.8733, datë 24.01.2001 "Për disa shtesa dhe ndryshime në Kodin Penal". Me anë të këtij ligji u parashikuan dy figura të reja të veprave penale në përgjigje të fenomeneve që ishin vërejtur në praktikë[89]. E para ishte vepra penale që parashikonte ndërhyrjet në transmetimet dhe programet kompjuterike dhe e dyta parashikonte prodhimin dhe përdorimin e sistemeve telematike, mjeteve dhe pajisjeve të teknologjisë së lartë, në rastet e veprave penale në fushën e narkotikëve ose për të mundësur ose lehtësuar konsumimin e lëndëve narkotike dhe psikotrope ose për të transmetuar a përhapur njoftime publicitare për stimulimin e përdorimit të tyre. Në kushtet që të vetme këto dy vepra penale ishin të pamjaftueshme për të luftuar kriminalitetin e shfaqur nëpërmjet teknologjisë në rritje, në vitin 2008 është kryer një tjetër reformë legjislative, e cila materializoi një sërë veprash të rëndësishme në kundërpërgjigje të fenomeneve shoqërisht të rrezikshme me bazë teknologjinë. Këtu duhet ritheksuar se bëhet fjalë për rastet e keqpërdorimit të teknologjisë dhe abuzimit me mundësitë që ajo mund të ofrojë, pra, të evidentimit në praktikë të rasteve të përdorimit të teknologjisë për kryerjen e veprimeve që paraqesin rrezik për shoqërinë, si mashtrimi, falsfikimi, kanosja, shpërndarja e materialeve raciste e ksenofobe, ndërhyrja në rrjetet apo të dhënat kompjuterike, por ende

---

personit pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet". Në nenin 123 të Kodit Penal parashikohej se: "*Kryerja me dashje e veprimeve të tilla si asgjësimi, mosdorëzimi, hapja dhe leximi i letrave apo çdo korrespondencë tjetër, si dhe ndërprerja ose vënia nën kontroll, dëgjimi i bisedave telefonike, telegrafike ose i çdo mjeti tjetër telekomunikimi, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet*.

8 Neni 192/b – *Ndërhyrja në transmetimet kompjuterike*: *Ndërhyrja në çdo formë, në transmetimet dhe programet kompjuterike, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në tre vjet. Po kjo vepër, kur ka sjellë pasoja të rënda, dënohet me burgim gjer në shtatë vjet.*

9 Neni 286/a – *Përdorimi i paligjshëm i teknologjisë së lartë*: *Prodhimi dhe përdorimi i sistemeve telematike, mjeteve dhe pajisjeve të teknologjisë së lartë, në rastet e veprave penale të parashikuara në nenet 283 gjer 286/a të këtij Kodi ose për të mundësuar ose lehtësuar konsumimin e lëndëve narkotike dhe psikotrope ose për të transmetuar a përhapur njoftime publicitare për stimulimin e përdorimit të tyre, dënohet me burgim gjer në pesë vjet*.

jo të parashikuara apo kriminalizuara si vepra penale. Këto ndryshime janë pasuar në vijim në vitet më pas edhe me ndërhyrje tëtjera legjislative. Me qëllim ilustrimin e efektit të së drejtës penale në ndjekjen e veprave penale me bazë teknologjinë kemi përzgjedhur të citojmë vendimin e Gjykatës së Lartë nr.261, datë 02.10.2013. Çështja i referohet kallëzimit të një subjekti juridik-platformë dixhitale që ofron shërbime mediatike, i cili ka pretenduar se nga persona të ndryshëm të cilët ushtrojnë aktivitet tregtar ne fushën e elektronikës, është mundësuar ndërhyrja në sistemin kompjuterik konkretisht internet duke realizuar shkatërrimin e kodeve e si rezultat, mundësimi i ofrimit në mënyrë të kundraligjshme i disa programeve, ekskluzivitetin e të cilave e ka pasur vetëm subjekti juridik kallëzues. Nga ky veprim i kundraligjshëm këtij subjekti i ishte shkaktuar dëm ekonomik. Faktet për këtë pjesë të kallëzimit u kualifikuan nga prokuroria dhe më pas gjykatat, si vepra penale e mashtrimit kompjuterik, parashikuar nga neni 143/b i Kodit Penal.Gjykata e Lartë arsyetoi lidhur me këtë vepër penale se: *Kjo vepër, nga ana objektive, është kryer në formën e ndryshimit të të dhënave kompjuterike, pasi aparati "Dreambox" që ata kanë shitur, funksionon duke përdorur një kartë Smart të abonuar, e cila është në gjendje të dekriptojë "çelësin" dhe më tej lidhet me internetin, duke bërë të mundur ndarjen e "çelësit/kodeve" në të gjitha aparatet e tjerë, të cilët nuk përdorin kartën Smart. Në momentin që klienti merr aparatin "Dreambox", pasi lidhet me sinjalin e internetit, merr çdo të dhënë kodesh nga "Dreambox" serveri dhe kështu përftohet pamja vizive. Karta Smart rezulton se është pjesë përbërëse e sistemit kompjuterik*[10].

Nga ana tjetër, duhet kuptuar se roli i teknologjisë në luftën dhe parandalimin e kriminalitetit, nuk qendron vetëm në faktin që kodi penal përpiqet në vazhdimësi të përmirësohet në luftën ndaj fenomeneve që abuzojnë me të mirat e teknologjisë, por teknologjia ndikon edhe në parandalimin e kryerjes së veprave të tjera penale, të cilat në dukje japin përshtypjen se nuk kanë lidhje me teknologjinë, të tilla si shpërdorimi i detyrës, korrupsioni, ushtrimi i ndikimit të paligjshëm, shkelja e barazisë në tendera, pastrimi i produkteve të veprës penale dhe veprimtarive kriminale etj. Sisteme elektronike/kompjuterike në insitucione të tilla si gjykata, prokurori, administrata publike, gjendje civile, zyrat e kadastrës etj., ndikojnë drejpërdrejtë në minimizimin e rasteve të shkeljeve të kryera gjatë detyrës nga zyrtarët publikë dhe të shkeljeve apo veprave të kryera nga individët.

10 Për më gjerë, citohet në vendimin e Gjykatës së Lartë nr. 261, datë 02.10.2013

3. Përqasja e Kodit të Procedurës Penale me zhvillimet e teknologjisë

Përmirësimi i Kodit të Procedurës Penale si efekt i zhvillimeve teknologjike duhet evidentuar në dy aspekte të ndryshme apo në dy grupe normash, së pari ato të cilat lehtësojnë veprime të caktuara procedurale apo faza të procesit penal dhe ato të cilat kanë të bëjnë me përdorimin e teknologjisë në marrjen e provave. Sigurisht që, të dyja këto aspekte kanë të njëjtin qëllim fundor që është zhvillimi i një procesi penal bashkëkohor.

Regjistrimi audio në proces dhe njoftimet e palëve.

Në grupin e parë të normave veçojmë ato që parashikojnë zhvillimin e procesit gjyqësor me regjistrim audio. Në nenin 115 të K.Pr.Penale, pas reformës legjislative të vitit 2017 parashikohet se: 1. *Kur është e mundur, aktet e kryera gjatë seancës gjyqësore, si dhe çdo akt tjetër i kryer jashtë saj, dokumentohen nëpërmjet regjistrimit audio ose audioviziv*. Regjistrimi audio ose audioviziv shoqërohet dhe me përpilimin e transkriptimeve të procesverbaleve të mbajtura në këtë formë.Vetëm pak përpara ndryshimeve të mësipërme legjislative, por ndërkohë kur kishte filluar aplikimi i sistemit audio në gjykatat e vendit, Gjykata e Lartë në vendimin unifikues nr.1, datë 27.04.2015 ka shprehur se: "(…) *mbajtja e procesverbalit të seancës gjyqësore nëpërmjet regjistrimit audio dhe audioviziv, është jo vetëm në përputhje me nenin 115 e vijues të K.Pr.Penale, por duke u parashikuar prej tij si një nga mjetet e mbajtjes së procesverbalit, rrit efektivitetin, eficiençën dhe garanton transparencën në seancat gjyqësore duke përmbushur në mënyrë shteruese dhe autonome funksionin dokumentues të veprimeve procedurale*"[11].

Në këtë grup normash, mund të citojmë edhe ato që kanë të bëjnë me mënyrën dhe mjetet për njoftimin e palëve të procesit. Në nenin 133 të K.Pr. Penale është parashikuar njoftimi me mjete të tjera teknike i personave që mund të jenë pjesë e procesit penal, përveç të pandehurit.Edhe përpara ndryshimeve legjislative të vitit 2017, në këtë dispozitë parashikohej njoftimi me telefon, telegraf dhe faks, duke pasur si kriter ligjor ngutshmërinë apo përshtatshmërinë e njoftimit.Aktalisht, dispozita është riformuluar në mënyrë të tillë qëpraktikisht njoftimi mund të bëhet me çdo mjet teknik, me kusht që të dokumentohet marrja e tij[12] dhe një mënyrë e tillë njoftimi

11 Për më gjerë, citohet në vendimin unifikues të Gjykatës së Lartë nr. 1, datë 27.04.2015

12 1. *Gjykata në raste të ngutshme mund të urdhërojë që personat e kërkuar nga palët, përveç të*

çmohet e përshtatshme nga gjykata.

Pyetja në distancë e subjekteve.

Përpos rëndësisë që paraqesin normat e mësipërme në ecurinë normale të procesit penal, vlerësojmë se ndikimi i teknologjisë në teknikat dhe mjetet e përftimit të provave në procesin penal përbën çështjen më të rëndësishme e përcaktuese në kryerjen e një procedimi të drejtë dhe efektiv. Një ndër elementët më të rëndësishëm të reformave legjislative të K.Pr.Penale ka qenë parashikimi i mundësisë së zhvillimit të pyetjes së subjekteve të procesit penal në distancë me mjete audiovizive, apo dhe regjistrimi i pyetjes me mjete audiovizive. Rrethi i subjekteve të cilët mund t'i nënshtrohen kësaj forme të realizimit të pyetjes, përbëhet nga bashkëpunëtorët e drejtësisë, personat e infiltruar ose personat nën mbulim, dëshmitarët e mbrojtur, dëshmitarët me identitet të fshehur, personi i marrë si i pandehur në një procedim të lidhur ose që vuan dënimin jashtë shtetit, viktimës së mitur, viktimës së abuzuar seksualisht dhe viktimës së trafikimit të qenieve njerëzore, si edhe çdo dëshmitar që parashikohet në nenin 361/7 të K.Pr.Penale[13]. Megjithatë, nga një konstatim i përgjithshëm i zbatueshmërisë së këtyre teknologjive në procesin penal, mund të thuhet se ende nuk kemi një historik apo përvojë të gjerë në përdorimin e tyre. Këtu ka ndikuar dhe infrastruktura e limitur e gjykatave për të aplikuar teknika të tilla në pyetjen e subjekteve. Gjithashtu, nga e njëjta problematikë e karakterizuar nga mungesa e infrastrukturës përkatëse teknike ka qenë e kushtëzuar edhe veprimtaria e Prokurorisë sa i përket pyetjes në distancë të subjekteve që parashikohen në ligjin procedural penal.

Pyetja e të miturve viktimë e veprës penale/dëshmitarë.

Rregulla më të hollësishme janë parashikuar për teknikat e pyetjes së të miturve viktimë apo dëshmitarë sipas Kodit të Drejtësisë Penale për të

pandehurit, të lajmërohen me telefon nga sekretaria e gjykatës ose nga policia gjyqësore. Në origjinalin e lajmërimit shënohet numri i telefonit të kërkuar, emri dhe detyra që kryen personi që merr njoftimin, marrëdhëniet e tij me atë që njoftohet,data dhe ora e telefonatës. 2. Njoftimi me telefon ka vlerë nga çasti kur është bërë, me kusht që të dokumentohet marrja e tij. 3. Shfuqizuar. 4. Gjykata, kur e çmon të përshtatshme, përveç të pandehurit, mund të disponojë njoftimin e personit, me mjete të tjera teknike që garantojnë njoftimin, me kusht që të dokumentohet marrja e tij. 5. Njoftimi i dëshmitarit me identitet të fshehur, dëshmitarit të mbrojtur dhe bashkëpunëtorit të drejtësisë bëhet nëpërmjet dorëzimit të kopjes së aktit prokurorit.

13 Shih nenet 58/a, 58/b, 165/a, 167/a, 361/7, 361/a dhe 361/b të Kodit të Procedurës Penale

Mitur[14]. Nga nenet 39 deri në nenin 42 të Kodit të Drejtësisë Penale për të Mitur janë parashikuar norma specifike për aplikimin e masave me karakter teknik gjatë pyetjes së të miturve viktimë të veprës penale, veçanërisht atyre që janë viktimë e shfrytëzimit ose dhunës sekuale. Në legjislacionin shqiptar është hera e parë që parashikohen rregulla të detajuara për pyetjen e të miturit viktimë dhe /ose dëshmitar i shfrytëzimit seksual ose dhunës seksuale. Sipas parashikimit ligjor të Kodit të Procedurës Penale para hyrjes në fuqi të ndryshimeve të tij të parashikuara në Ligjin nr.35/2017, datë 30.03.2017, si dhe para hyrjes në fuqi të Kodit të Drejtësisë Penale për të Mitur pyetja e të miturit pavarësisht nga mosha e tij kryhej sipas rregullimeve të nenit 361 të KPP. Konkretisht, i mituri pyetej nga kryetari i trupit gjykues duke u asistuar nga një psikolog ose familjar i të miturit dhe në prani të palëve në proces, pasi nuk kishte ndalesë në këtë drejtim. Nëse çmohej nga gjykata se pyetja e drejtpërdrejtë e të miturit nuk dëmtonte gjendjen psikologjike të tij, pyetja e tij bëhej nga vet palët në proces, prokurori dhe i pandehuri dhe mbrojtesi i tij/saj. Sipas praktikës gjyqësore në raste të gjykimit të veprave penale të kryerjes së marrëdhënieve seksuale me të mitur pyetja e të miturve është zhvilluar përmes psikologut në ambiente të veçuara nga salla e gjykimit përmes videokonferencës duke siguruar në këtë mënyrë mungesën e kontaktit të të pandehurit me të miturin viktimë të veprës penale, siç ka ndodhur në rastin e çështjes penale *Prokuroria kundër David Broën* dënuar për veprën penale "kryerja e marrëdhënieve seksuale me të mitur" viti 2008[15]. Nga pikëpamja procedurale parashikimi nenit 41/1 fjalia e dytë e Kodit të Drejtësisë Penale për të Mitur, sipas të cilit, për këta të mitur[16], regjistrimi audio dhe video gjatë pyetjes është i detyrueshëm, paraqet rëndësi, pasi është një detyrim që nuk lejon asnjë përjashtim.

Teknologjia dhe ekspertimi.

Përpos, pyetjes së subjekteve të procesit penal, si një ndër provat e rëndësishme të procesit, të trajtuara më lart, prova me ekspertim, futet në kategorinë e atyre provave, ku impakti i teknologjisë është më i ndjeshëm dhe i drejtpërdrejtë. Kjo për shkak se ka një raport të drejtë ndërmjët teknologjisë së përparuar në kryerjen e ekspertimeve dhe cilësisë e garancisë së tyre në procesin penal.Madje, këtë karakter e ka pranuar edhe vetë Kodi i Procedurës Penale në nenin 178/1 të tij kur ka parashikuar se:

14 Miratuar me Ligjin nr.37, datë 30/03/2017

15 http://komentarielektronik.magjistratura.edu.al/sq/eli/fz/2017/37/41

16 Të miturit viktimë dhe/ose dëshmitar, të shfrytëzimit seksual ose dhunës seksuale

"Ekspertimi lejohet kur është i nevojshëm zhvillimi i kërkimeve ose marrja e të dhënave ose e vlerësimeve që kërkojnë njohuri të posaçme teknike, shkencore ose kulturore. Në Kodin e Procedurës Penale nuk përcaktohen apo listohen kategoritë konkrete të ekspertimeve që mund të kryhen nga organi procedues. Kjo do të thotë që ligjvënësi llojet konkrete të ekspertimeve i ka konsideruar pjesë të fushës së kriminalistikës, mjekësisë apo shkencave natyrore dhe në vlerësimin tonë jo pa qëllim, duke pasur në konsideratë se ato janë të lidhura drejtpërdrejtë me zhvllimin e teknologjisë.

Nga pikëpamja juridike dhe procedurale penale, duke pasur në konsideratë vështirësinë e të provuarit, kryesisht të veprave të rënda penale, në praktikën hetimore dhe gjyqësore me rëndësi të posaçme janë ekspertimet e ADN-së dhe ato kompjuterike. Ekspertimet e ADN-së, si ato biologjike me qëllim ekstraktimin/identifikimin e ADN-së nga provat materiale të gjetura në një vendngjarje dhe ato për krahasimin e saj me bazën e të dhënave që disponon Instituti i Policisë Shkencore (me qëllim identifikimin e personit) kanë dhënë një ndihmesë të çmuar në hetimin e veprave penale të drejtuara ndaj jetës dhe shëndetit të personave. Më specifik është rasti i ekspertimit biologjik që nevojitet të kryhet ndaj një personi. Në këtë rast,mbi bazën e ndalimeve në lidhje me rrethanat rreth privatësisë që i përkasin secilit individ, ligjvëvësi normon përmes dispozitës së Nenit 201/a të K.Pr.Penale (dispozitë kjo e shtuar me ligjin 35/2017) procedurat që duhet të ndiqen për marrjen me qëllim ekspertimi të kampioneve biologjikë. Urdhërimet e kësaj dispozite u përkasin si rasteve kur kampionet biologjikë merren pa vullnetin e personit (me detyrim), ashtu edhe kur merren me vullnetin e tij, që duhet të jepet me shkrim (& 2 i Nenit 201/a). Kampionet biologjikë mund të merren me detyrim vetëm me vendim gjyqësor, si atëhere kur personi është në gjëndje të lirë, ashtu edhe kur është me masë sigurimi arrest në burg apo i ndaluar proceduralisht[17].

Ekspertimet kompjuterike, duke marrë në konsideratë gamën e gjerë të pajisjeve teknologjike, kanë shërbyer veçanërisht për hetimin e veprave penale, ku vetë teknologjia është përdorur si mjet për kryerjen e veprës penale, e këtu kemi parasysh veprat penale në fushën kompjuterike/ elektronike, krimin kibernetik etj., dhe për ato vepra penale, për të cilat është i nevojshëm ekspertimi kompjuterik i provave materiale si kompjutera, telefona, karta telefonike, USB etj. Me qëllim ilustrimin e rëndësisë së këtyre ekspertimeve, më konkretisht bëhet fjalë për ekspertimin teknik kompjuterik paraqesim një rast të gjykuar nga

17 http://avokatia.al/revista/20-avokatia-34/78-penale-34, Spiro Spiro, Doktrina dhe legjislacioni procedural penal mbi ekspertimet, në Revista Avokatia, Nr.34.

Gjykata e Lartë me vendimin nr.173, datë 21.10.2015. Nga rrethanat e çështjes ka rezultuar se të pandehurit janë akuzuar për kryerjen e veprave penale të *Hyrja e paautorizuar kompjuterike", "Ndërhyrja në sistemet kompjuterike"dhe "Keqpërdorimi i pajisjeve", bazuar ne nenet 192/b-1, 293/c-1, 293/ ç të Kodit Penal.* Nga hetimet e kryera ka rezultuar se të pandehurit kishin përdorur metodën "Phishing"[18], për të vjedhur të dhënat personale të shumë individëve. Lidhur me këtë rast, nga gjykatat është arsyetuar, arsyetim i mbështetur edhe nga Gjykata e Lartë se: "*nga analiza e provave te administruara ne fashikullin e hetimit rezulton plotësisht e provuar se te pandehurit me veprimet e kundraligjshme, të kryera nëpërmjet hyrjes së paautorizuar në sistemin kompjuterik të rrjetit social Facebook apo dhe rrjeteve të tjera, nëpërmjet cënimit dhe vjedhjes së fjalëkalimeve të përdoruesve të këtyre sistemeve, ndërhyrjes në sistemet kompjuterike të subjekteve shtetërore dhe private brenda dhe jashtë Shqipërisë si dhe duke keqpërdorur (mbajtur dhe përdorur pajisjet dhe programet kompjuterike), me qëllim kryerjen e krimeve të sipërcituara, kanë konsumuar elementët e veprave penale "Hyrja e pa autorizuar kompjuterike", parashikuar nga neni 192/b/1, "Ndërhyrja në sistemet kompjuterike", parashikuar nga neni 293/1/c i K.Penal, dhe "Keqpërdorimi i pajisjeve", parashikuar nga neni 293/ç i K.Penal*[19]

Provat me dokument dhe mjetet e kërkimit të proves.

Interes paraqesin edhe disa lloje provash dhe mjete të kërkimit të provës, të cilat janë përshtatur në mënyrë të tillë që t'i përgjigjen njëkohësisht edhe zhvillimeve të teknologjisë. Në seksionin e dokumenteve janë parashikuar të dhënat kompjuterike të memorizuara në një sistem kompjuterik apo në një mjet tjetër memorizimi. Lidhur me mënyrën e marrjes dhe administrimit të tyre është parashikuar një procedurë e posaçme[20]. Në sekuestrimet si

18 "*Phishing*", *është akti i tentimit për kopjimin e informacionit si "emri i përdoruesit", "fjalëkalimet", etj, nëpërmjet kamuflimit si entitete ligjore gjatë komunikimit elektronik në adresa interneti popullore dhe sociale, adresa për kryerjen e ankandeve etj, të cilat përdoren kryesisht për të joshur publikun që nuk dyshon. Mesazhet elektronike "Phishing", mund të përmbajnë lidhje Interneti me adresa të cilat janë të infektuara me virus kompjuterik. Kjo metodë kryhet kryesisht nëpërmjet mesazheve elektronike të rreme apo komunikime "Chat" dhe shpesh i drejton përdoruesit të japin detajet e tyre tek një faqe interneti e falsifikuar, të cilat kanë pamjen e atyre legjitime*, citim nga vendimi i Gjykatës së Lartë nr. 173/2015

19 Vendimi i Gjykatës së Lartë nr. 173, datë 21.10.2015

20 Neni 191/a Detyrimi për paraqitjen e të dhënave kompjuterike (Shtuar me ligjin nr.10 054, datë 29.12.2008): Gjykata, në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, me kërkesë të prokurorit ose viktimës akuzuese urdhëron mbajtësin ose

mjet kërkimi prove, janë parashikuar, gjithashtu, procedura të posaçme për sekuestrimin e të dhënave kompjuterike ose sistemeve kompjuterike[21]. Emëruesi i përbashkët i këtyre dispozitave është se kryerja e sekuestrimeve është e lidhur me ekzistencën e veprave penale që kanë të bëjnë me teknologjinë e informacionit. Rëndësi si mjet kërkimi prove paraqet edhe përgjimi, për të cilin ligji parashikon se mund të kryhet me çdo mjet teknik, me kushtin e respektimit të procedurës përkatëse, veçanërisht roli i gjykatës në vlerësimin e kërkesës për pranimin e përgjimit, si një garantuese e të drejtës për privatësi të individit. Deri aktualisht, në praktikën hetimore dhe gjyqësore është i njohur përgjimi 'klasik' telefonik dhe janë të rralla rastet e përgjimeve të natyrave të ndryshme, si përdorimet e mjeteve për përgjimin e aplikacioneve dhe rrjeteve sociale, mjetet teknike për përcaktimin e vendndodhjes së individit dhe automjetit, përdorimi i videos gjatë vëzhgimeve apo përdorimi i dronëve etj.

4. Përfundime

Vlerësojmë se përmirësimi i teknikave dhe mjeteve për marrjen dhe administrimin e provave, si edhe ato që kanë lidhje me rrjetet dhe sistemet kompjuterike, do të ndikojë drejtpërdrejtë në realizimin e një procedimi të drejtë e të paanshëm penal, si në drejtim të luftës ndaj kriminalitetit, ashtu edhe në drejtim të respektimit të të drejtave të individit gjatë procesit penal. Ajo që shihet si e nevojshme në realitetin e vendit tonëështë pasurimi i infrastrukturës teknike të shërbimeve të policisë gjyqësore, prokurorisë dhe gjykatës me mjetet e nevojshme teknologjike për kryerjen e detyrimeve përkatëse ligjore në këtë fushë. Megjithatë, këto elementë mund të rezultojnë të pamjaftueshëm, nëse institucionet e drejtësisë nuk bashkëpunojnë në këtë fushë edhe me institucione të tjera të specializuara, universitetet apo dhe kompanitë private, të dhënat dhe informacionet e të cilëve mund të jenë të rëndësishme për procese të caktuara. Nga pikëpamja juridiko-penale është e rëndësishme të theksohet se kodi penal ka nevojë të azhornohet në vazhdimësi me veprat penale, të cilat lindin si rezultat i keqpërdorimit të teknologjisë. Këtu bëhet fjalë për disa fenomene shoqërisht të rrezikshme, të

kontrolluesin të dorëzojnë të dhënat kompjuterike të memorizuara në një sistem kompjuterik apo në një mjet tjetër memorizimi. Gjykata, në këto procedime, urdhëron edhe dhënësin e shërbimit për dorëzimin e çdo informacioni për abonentët e pajtuar, për shërbimet e ofruara nga dhënësi. Kur ka arsye të bazuara për të menduar se nga vonesa mund t'u vijë një dëm i rëndë hetimeve, prokurori vendos, me akt të motivuar, detyrimin për paraqitjen e të dhënave kompjuterike, të përcaktuara në pikat 1 e 2 të këtij neni dhe njofton menjëherë gjykatën. Gjykata vlerëson vendimin e prokurorit brenda 48 orëve nga njoftimi.

21 Për më gjerë shih nenet 208/a, 299/a dhe 299/b të K.Pr.Penale.

cilat nuk gjejnë pasqyrimin e duhur në kodin penal dhe interpretimi i normave aktuale nuk është shumë adekuat me parimet që udhëheqin zbatimin e së drejtës penale si mosaplikimi i ligjit me analogji, apo interpretimi i zgjeruar në drejtim të keqësimit të pozitës së të dyshuarit. Këto fenomene përfshijnë, por nuk kufizohen vetëm me to, shfrytëzimi seksual i fëmijëve në internet, tregtia online e mallrave të paligjshme, mashtrimi me kriptomonedhat etj.

Bibliografia

Baccari Gian Marco, Conti Calotta, *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, në Diritto Penale e Processo, Mensile di giurisprudenza, legislazione e dottrina, Nr.6/2021,

Cesari Claudia, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, në Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1167-1188, set.-dez. 2019,

Nardi Valérie, *I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider*, në Diritto Penale Contemporaneo, 2019,

Pezzuto Raffaella, *Contenuti terroristici on-line: L'Unione Europea lavora a nuove forme per prevenirne la diffusione*, në Diritto Penale Contemporaneo, Rivista Trimestrale, Nr.4/2019,

Spangher Giorgio, *Covid-19: nel disastro si vede chiaro*, në Penale Diritto e Procedura, Rivista trimestrale, Nr.1/2020

Spiro Spiro, *Doktrina dhe legjislacioni procedural penal mbi ekspertimet*, Revista Avokatia, Nr.34,

Ubertis Giulio, *Giustizia penale e nuove tecnologie*, në Diritto Penale Contemporaneo, Rivista Trimestrale, Nr.4/2020

- Vendimi i Gjykatës së Lartë nr.261, datë 02.10.2013
- Vendimi unifikues i Gjykatës së Lartë nr.1, datë 27.04.2015
- Vendimi i Gjykatës së Lartë nr.173, datë 21.10.2015

http://komentarielektronik.magjistratura.edu.al/sq/eli/fz/2017/37/41

http://avokatia.al/revista/20-avokatia-34/78-penale-34

https://archiviodpc.dirittopenaleuomo.org/upload/4923-nardi2019a.pdf

- Kodi Penal
- Kodi i Procedurës Penale
- Kodi i Drejtësisë Penale për të Mitur

LEGAL ISSUES OF CYBERSECURITY IN ELECTIONS

DR. ADA GÜVEN –HAJNAJ

Department of Law, "Bedër" University College

aguven@beder.edu.al

Abstract

The last decade has marked an increased usage of new technologies in elections, that has raised concerns on free, fair and true elections and thus the trust in democracy. As electoral processes are relying more frequently on the internet, technological devices and software, the more are becoming target of cyber-attacks. Countries persistently are using these technologies, so the need for an effective frameëork for protecting against cyber threats has never been greater.

The paper will discuss the concept of electronic voting systems, the various types that are used such as voting with a direct-recording machine or internet voting that refers to the usage of the Internet to cast or transmit the vote. All the types of electronic voting systems can take different forms conditioned by the environment that it is being held and are regulated by a specific legal framework provided in the respective legislations. The paper will analyze the electronic voting, the international principles and standards to be respected for the very reason that elections are considered to be an essential component in achieving democracy.

Furthermore, the article will analyze specifically the Budapest Convention on Cybercrime whereas EU countries agree that interference with elections through malicious cyber activities against computers and data used in elections should be handled in much more effective manner. This convention provides that such cyber-attacks and interferences should be prosecuted

in case they constitute a criminal offence with purpose of reassuring the electorate with regard to the use of information and communication technologies in elections.

***Key words**: elections, cybersecurity, democracy, electronic voting systems.*

1. Hyrje: Sistemet elektronike të votimit

Dekada e fundit ka shënuar një rritje të përdorimit të teknologjive të reja në zgjedhje, gjë që ka ngritur shqetësimin për zgjedhje të lira, të ndershme dhe si rrjedhim besimin në demokraci. Ndërsa proceset zgjedhore po mbështeten më shpesh në internet, pajisje teknologjike dhe programe kompjuterike, aq më shumë po bëhen objektiva e sulmeve kibernetike. Shtetet po i përdorin vazhdimisht këto teknologji, kështu që nevoja për një kornizë efektive për mbrojtjen nga kërcënimet kibernetike nuk ka qenë kurrë më e madhe. Kornizat rregullatore duhet të trajtojnë ndër të tjera strategjitë e rrezikut, masat mbrojtëse, mundësitë e verifikimit dhe planifikimin e emergjencës, Në lidhje me sa më lart, udhëzimet ekzistojnë në nivel rajonal, bazuar në instrumentet ligjore ndërkombëtare që trajtojnë sigurinë kibernetike. Komiteti i Këshillit të Evropës, në lidhje me Konventën e Budapestit për krimin kibernetik, ka nxjerrë një shënim udhëzues për zgjedhjet i cili trajton përdorimin e kompetencave procedurale të Konventës së Budapestit dhe dispozitave të ndihmës juridike reciproke në një hetim penal specifik ose procedim në ndërhyrje në zgjedhje.

Implemetimi i votimit me anë të sistemeve elektronike çon në rritjen e numrit të votuesve në gjithashtu mbart premtimin për për forcimin e efikasitetit në procesin zgjedhor dhe shpresën për afrimin e votuesve me përfaqësuesit e tyre. Në kontekstin aktual në të cilin, në shumë demokraci perëndimore vihet re një ulje e pjesëmarrjes në votime dhe zhgënjimit të votuesve në shkallë të gjerë ndaj politikës, politikëbërësit kanë kërkuar strategji novatore për të ringjallur interesin dhe besimin e qytetarëve si dhe për të promovuar një proces demokratik me pjesëmarrje[1].

Votimi elektronik është një risi veçanërisht tërheqëse në këtë drejtim, në kuptimin që kombinon teknologjinë në thelbin e pjesëmarrjes demokratike. Megjithatë, vihet re që si rastet e suksesshme ashtu edhe ato të pasuksesshme

1 International IDEA. (2011). *Introducing Electronic Voting: Essential Considerations* Stockholm: INTERNATIONAL IDEA.Fq. 6, aksesuar më 07 korrik 2022.

të përpjekjeve për të zhvilluar zgjedhje me anë të sistemeve elektronike po zbulojnë gjithnjë e më tepër, kompleksitetin që lidhet me një procedurë plotësisht funksionale të votimit elektronik. Nga njëra anë, votimi elektronik ofron shumë avantazhe të mundshme si lehtësimi i procesit të votimit, lehtësia e shtuar për votuesit, përfitimet në efikasitet dhe premtimi i rritjes së përqindjes së pjesëmarrjes në plan afatgjatë. Ndërkohë që nga ana tjetër, ajo gjithashtu vjen me sfida të shumta të cilat, nëse nuk trajtohen siç duhet, mund të minojnë integritetin e zgjedhjeve. Shqetësimet teknologjike dhe të sigurisë shpesh përmenden si kërcënimet kryesore për votimin në internet. Megjithatë, kërkimet e fundit tregojnë se shumimi i pilotëve, testeve dhe numrit të zgjedhjeve me e-aktivitet ka një kontribut vendimtar për zhvillimin e sistemeve më të sigurta të votimit elektronik[2].

Sfidat ligjore lidhen me faktin se votimi elektronik duhet të konceptohet brenda kuadrit më të gjerë të legjislacioneve zgjedhore kombëtare. Ndërkohë në planin e Bashkimit Evropian (BE), marrja e një zgjidhjeje uniforme në të gjithë Shtetet Anëtare është më sfiduese, prandaj zgjidhja optimale duket se konsiston në një qasje të decentralizuar ku Shtetet Anëtare veprojnë brenda kufijve kufizues të një ligji zgjedhor gjithëpërfshirës evropian. Në këtë drejtim, Reforma e Ligjit Evropian Zgjedhor është një kontribut i rëndësishëm për harmonizimin e procedurave zgjedhore në të gjitha shtetet anëtare.

Votimi elektronik tashmë ka kaluar fazën e provës dhe është duke u përhapur gradualisht me rezultate të suksesshme në të gjithë vendet evropiane si dhe përtej kufijve të Evropës. Megjithatë, studiesit janë të pikëpamjes që, nëse votimi elektronik vihet në dispozicion të votuesve, atëherë duhet të propozohet si një alternativë ndaj votimit më anë të fletëvotimit.

Punimi do të diskutojë konceptin e sistemeve të votimit elektronik, llojet e ndryshme që përdoren si votimi me një makinë regjistrimi të drejtpërdrejtë ose votimi në internet që i referohet përdorimit të internetit për të hedhur ose transmetuar votën. Të gjitha llojet e sistemeve të votimit elektronik mund të marrin forma të ndryshme të kushtëzuara nga mjedisi që zhvillohet dhe rregullohen nga një kuadër ligjor specifik i parashikuar në legjislacionin përkatës. Punimi do të analizojë votimin elektronik, parimet dhe standardet ndërkombëtare që duhen respektuar pikërisht për arsyen se zgjedhjet konsiderohen si një komponent thelbësor në arritjen e demokracisë.

2 Ben Goldsmith, Holly Ruthrauff. (n.d.). *Case Study Report on Electronic Voting in the Netherlands.* Retrieved from NDI, Implementing and Overseeing Electronic Voting and Counting Technologies: https://www.ndi.org/sites/default/files/5_Netherlands.pdf. Fq. 25 aksesuar më 07 korrik 2022.

2. Llojet e votimit elektronik

Votimi elektronik (E-Voting) si term përfshin një gamë të gjerë sistemesh votimi që aplikojnë elemente elektronike në një ose më shumë hapa të ciklit zgjedhor. Ky fokus po përqendrohet në sistemet që mbështesin një ose më shumë nga hapat e mëposhtëm në procesin e zgjedhjeve ose referendumit në mënyrë elektronike: regjistrimi, hedhja dhe/ose numërimi i votave.

Duhet bërë një dallim shumë themelor midis sistemeve të votimit elektronik që zbatohen në mjedise të kontrolluara (a) dhe sistemeve të votimit elektronik që zbatohen (pjesërisht) në mjedise të pakontrolluara (b):

a. Sistemet e votimit elektronik në mjedise të kontrolluara

Këto sisteme përfshijnë forma të tilla si votimi me skanime optike dhe makineri të votimit elektronik me regjistrim të drejtpërdrejtë (makineri votimi DRE).

Fillimisht janë aplikuar sistemet e skanimit optik të votimit që parashikonte si procedurë që votuesi të vendoste shenjë optike në letrën e votimit (e cila mund të jetë digitale ose letër specifike e skanueshme) dhe të lexohej nga një skaner elektronik i votimit[3].

Ky lloj sistemi karakterizohet nga fakti se votimi po zhvillohet në një vend të mbikëqyrur fizikisht, pra në një qendër votimi të vrojtuar nga përfaqësues të qeverisë ose autoriteteve të pavarura zgjedhore. Karakteristikat elektronike të makinës së votimit DRE është regjistrimi i votave me anë të një ekrani të fletëvotimit të pajisur me komponentë mekanikë ose elektro-optikë që mund të aktivizohen nga zgjedhësi. Këto janë zakonisht butona ose një ekran me prekje. Këo pajijse përpunojnë të dhëna duke përdorur një program kompjuterik për të regjistruar të dhënat e votimit dhe imazhet e fletëvotimeve në komponentët e memories. Në perfundim të zgjedhjeve pajisja prodhon një tabelë të të dhënave të votimit të ruajtura në një komponent memorie të lëvizshme dhe si kopje të printuar. Sistemi mund të ofrojë gjithashtu një mjet për transmetimin e fletëvotimeve individuale ose totalit të votave në një vend qendror për konsolidimin dhe raportimin e rezultateve nga njësitë në vendndodhjen qendrore[4].

Ky lloj sistemi filloi të përdorej masivisht në vitin 1996 në Brazil dhe me

3 International IDEA. (2011). *Introducing Electronic Voting: Essential Considerations* Stockholm: INTERNATIONAL IDEA.Fq. 6, aksesuar më 07 korrik 2022.

4 Ben Goldsmith, Holly Ruthrauff. (n.d.). *Case Study Report on Electronic Voting in the Netherlands.* Retrieved from NDI, Implementing and Overseeing Electronic Voting and Counting Technologies: https://www.ndi.org/sites/default/files/5_Netherlands.pdf. Fq. 25, aksesuar më 07 korrik 2022.

pas ne SHBA, ndërkohë që në Evropë filloi aplikimin për herë të parë në vitin 1989 në Hollandë ku dhe gjeti zbatim deri në vitin 2006. Në vitin 2007 u ndalua përdorimi i këtij sistemi sepse hakerët hollandezë dhe gjermanë demonstruan se një makinë votimi Nedap mund të mësohej të luante shah duke rregulluar softuerin e saj, pra demostruan se softueri mund të ndryshohej sipas dëshirës pa autorizim[5].

Ndërkohë, në Gjermani në vitin 2009 Gjykata Kushtetuese Federale shpalli Urdhëresën Federale të Makinerisë së Votimit si jokushtetuese "*sepse nuk siguron miratimin dhe përdorimin e vetëm atyre makinave të votimit që plotësojnë parakushtet kushtetuese që hapat kryesorë në procesin zgjedhor dhe përllogaritja e rezultateve të mund të inspektohen nga qytetarët në mënyrë të besueshme dhe pa pasur nevojë për njohuri të specializuara*"[6].

Gjykata vuri në dukje se, sipas kushtetutës, zgjedhjet kërkohet të jenë publike në natyrë dhe se të gjithë hapat thelbësorë të zgjedhjeve i nënshtrohen mundësisë së shqyrtimit publik, përveç rasteve kur interesat e tjera kushtetuese justifikojnë një përjashtim. Duke bërë të qartë se vendimi i gjykatës nuk përjashtonte në parim përdorimin e makinerive të votimit, ajo deklaroi se: *"Legjislativi nuk pengohet të përdorë makineritë elektronike të votimit në zgjedhje, nëse ruhet mundësia e një ekzaminimi të besueshëm të korrektësisë, e përcaktuar me Kushtetutë. Një ekzaminim plotësues nga zgjedhësi, nga organet zgjedhore ose nga publiku i gjerë është i mundur për shembull me makineritë elektronike të votimit në të cilat votat regjistrohen në një mënyrë tjetër përveç ruajtjes elektronike*."[7]. Ky vendim i Gjykatës Kushtetuese gjermane, duke theksuar nevojën për transparencë në procesin zgjedhor pa njohuri teknike të specializuara, i dha fund efektivisht përdorimit të fundit të votimit elektronik nga Gjermania. Megjithëse vendimi i Gjykatës nuk përjashton tërësisht makinat e votimit elektronik, nuk janë bërë lëvizje të mëtejshme për të adoptuar makineritë që plotësojnë kërkesat e transparencës[8].

b. Votimi elektronik në mjedise të pakontrolluara

Ky lloj votimi nënkupton që votimi mund të bëhet kudo jashtë qendrës së

5 Po aty

6 NDI. (2013, December 17). *The Constitutionality of Electronic Voting in Germany*. Retrieved from National Democratic Institute- Implementing and Overseeing Electronic Voting and Counting Projects: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany Aksesuar 27 korrik 2022.

7 Po aty.

8 Po aty.

votimit, p.sh. nje votues mund te perdore voten e tij nga shtepia nepermjet kompjuterit personal. Vota më pas transmetohet përmes internetit (në tekstin e mëtejmë të referuar si votim në distancë në internet), televizionit, telefonit ose rrjetit të telefonisë celulare. Përpos faktit që kjo metodë ofron përparësitë më të mëdha për votuesit, paraqet shqetësime më të mëdha të ruajtjes se sigurisë. Për vetë faktin se përfshijnë dyshime në lidhje me internetin si një mjet për transmetimin e informacionit konfidencial, frikë nga sulmet e hakerëve dhe ankthin për mundësinë e ndikimit të padrejtë që do të ushtrohet mbi votuesin gjatë procesit të votimit[9].

Një formë tjetër e votimit elektronik në një mjedis pjesërisht të pakontrolluar është votimi në kioskë. Me këtë, makina e votimit vendoset në një vend publik dhe komponentët e harduerit dhe softuerit kontrollohen nga zyrtarët zgjedhorë[10].

Dallimi ndërmjet këtyre metodave qëndron në faktin e kontrollit dhe vërtetimit të identitetit të votuesve, ku në votimin nëpërmjet internetit nuk është nën kontrollin e zyrtarëve zgjedhore ndërkohë në votimin me mjete të tjera elektronike procesi rregullohet dhe koordinohet nga zyrtaret zgjedhorë.

c. Sisteme me ose pa vërtetim të votuesve

Sistemet e votimit elektronik kanë disa karakteristika ku, disa sisteme të votimit elektronik përdoren vetëm për të dhënë votën dhe vërtetimi i votuesve kryhet në mënyrë manual, ndërkohë ka disa sisteme të tjera përmbajnë një modul shtesë për vërtetimin e votuesve bazuar në një regjistër elektronik të votimit ose në regjistrin zgjedhor[11]. Të gjitha sistemet e votimit në internet dhe disa makineri votimi në qendrat e votimit përmbajnë një modul vërtetimi.

Një sistem votimi që kryen të dy funksionet, atë të identifikimit të votuesve dhe përdorimin e votes, në thelb ka qënë objekt i kritikave dhe potencialisht ndaj keqpërdorimeve. Një sistem i tillë votimi edhe kur të dy funksionet mbahen posaçërisht të ndara nga njëra-tjetra, mund të ketë mundësi që operatorët e brendshëm të kontrollojnë të dy grupet e të dhënave. Kjo mundësi kërkon vendosjen e masave specifike teknike dhe procedurale

9 Kare Vollan. (2006). Voting in uncontrolled environment and the secrecy of the vote. *Electronic Voting 2006, 2nd International Workshop, Co-organized by Council of Europe* (pp. 155-169). Bregenz, Austria: Council of Europe.Fq. 159.

10 International IDEA. (2011). *Introducing Electronic Voting: Essential Considerations* . Stockholm: INTERNATIONAL IDEA, Fq. 7, Aksesuar 27 korrik 2022.

11 International IDEA. (2011). *Introducing Electronic Voting: Essential Considerations* . Stockholm: INTERNATIONAL IDEA, Fq. 12, Aksesuar 28 korrik 2022.

të sigurisë për të garantuar që këto dy grupe informacioni nuk mund të lidhen në asnjë rrethanë. Fshehtësia e votës mbështetet në këto masa dhe është e rëndësishme që ato të komunikohen dhe demonstrohen qartë tek palët e interesuara[12].

Pra, diskutimi akademik përfshin metodën e votimit elektronik, përdorimi i votës, numërimi i votave, ruajtja dhe përcjellja e informacionit pranë Komisionit Qendror të Zgjedhjeve (KQZ). Të gjitha këto hapa janë të rrezikuara nga ana kibernetike.

3. Instrumentet ndërkombëtare mbi zgjedhjet /Kuadri ligjor ndërkombëtar mbi zgjedhjet

Një nga çështjet kryesore kur studiohen sistemet elektronike të votimit është përputhshmëria me standartet demokratike dhe respektimi i të drejtave të njeriut si dhe parimet kryesore që janë parashikuar në instrumentet ndërkombëtare mbi zgjedhjet. Për vetë faktin se shkelja e këtyre parimeve dhe standarteve jetike gjatë realizimit të votimit elektronik, do të përkthehet në shtrembërim të vullnetit të votuesve dhe në zgjedhje të padrejta. Në këtë seksion do të analizojmë instrumentat ndërkomvëtarë mbi zgjedhjet dhe kriteret që kanë vendosur institucionet dhe organizatat ndërkombëtare të cilat sigurojnë respektimin e parimeve kryesore të zgjedhjeve që ndikojnëdrejtpërdrejtë në demokraci.

Një nga dokumentet më të rëndësishëm në këtë fushë është Paktin Ndërkombëtar të OKB-së për të Drejtat Civile dhe Politike, që është ratifikuar nga të gjitha shtetet anëtare të Këshillit të Evropës, ndërkohë që vetëm tre shtete anëtare të Këshillit të Evropës nuk kanë ratifikuar Protokollin № 1 të Konventës[13]. Zvicra dhe Monako e kanë nënshkruar por nuk e kanë ratifikuar deri më tani. Dispozitat ndërkombëtare zakonisht ofrojnë standarde minimale të cilat respektohen dhe tejkalohen nga ligjet kombëtare. E drejta ndërkombëtare detyruese përfshin nenin 21 të Deklaratës Universale të të Drejtave të Njeriut të Kombeve të Bashkuara të vitit 1948 (DUDNj), nenin 25 të Konventës Ndërkombëtare të OKB-së për të Drejtat Civile dhe Politike

12 Susanne Caarls. (2010, November). *E-voting Handbook: Key Steps for Introducing E-voting.* Retrieved from Council of Europe: https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf, Aksesuar 28 korrik 2022.

13 United Nations. (1966, December 16). *International Covenant on Civil and Political Rights*. Retrieved from UNHCR, Human Rights Instruments: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, Aksesuar 28 korrik 2022.

të vitit 1966 dhe nenin 3 të Protokollit № 1 të Konventës për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore siç interpretohet nga Gjykata Evropiane për të Drejtat e Njeriut[14].

Gjatë dekadës së fundit ka pasur një përpjekje të bashkërenduar brenda Këshillit të Evropës për të zhvilluar standardet per perdorimin e teknologjive te reja ne votime. Në vitin 2004, Komiteti i Ministrave i Këshillit të Evropës nxori Rekomandimin e tij mbi Standardet ligjore, Operacionale dhe Teknike për Votimin Elektronik. i cili përbën të parin dokument juridik ndërkombëtar të specializuar në këtë drejtim[15]. Ky rekomandim njohu rëndësinë e sigurimit që proceset e votimit elektronik të jenë të vëzhgueshme. Ndërkohë qe Standardet e Këshillit janë shpesh të natyrës teknike, duke theksuar ato aspekte të votimit elektronik që mund të tejkalojnë qëllimin e një misioni vëzhgimi ose vlerësimi të zgjedhjeve[16].

Ky rekomandim u pasua nga Raporti i Komisionit të Venecias mbi "Kompatibilitetin e votimit në distancë dhe të votimit elektronik me standartet e Këshillit të Evropës" në të cilin u analizua përputhshmëria e votimit elektronik me Nenin 3 të Protokolllit nr.1 të Konventës Evropiane për të Drejtat e Njeriut dhe Kodi i Praktikës së Mirë të Komisionit të Venecias në çështjet zgjedhore[17] Udhëzimi I.3.2 i Kodit shprehet se votimi elektronik duhet të pranohet vetëm nëse është i sigurt dhe i besueshëm. Theks të veçantë i vihet garantimit të transparencës së sistemit elektronik, sepse është një nga faktorët kryesorë që tragon për ruajtjen sa më të mirë të sistemit nga ndërhyrjet nga jashtë. Për këtë, zgjedhësit duhet të jenë në gjendje të marrin

14 Alexander H. Trechsel, Vasyl Kucherenko, Frederico Silva, Urs Gasser. (2016, May). *Potential and Challenges of e-voting in the European Union.* Retrieved from European Parliament, Directorate-General for Internal Policies, Policy Department, Citizen's Rights and Constitutional Affairs: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf, Fq. 8, Aksesuar 30 korrik 2022.

15 Committee of Ministers, Council of Europe. (2004, September 30). *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.* Retrieved from Committee of Ministers, Rec(2004)11: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp, Aksesuar 30 korrik 2022.

16 Committee of Ministers, Council of Europe. (2017, June 14). *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting.* Retrieved from Committee of Ministers, CM/Rec(2017)5 : https://rm.coe.int/0900001680726f6f, Aksesuar 02 gusht 2022.

17 Venice Commission . (2004, March 12-13). *CDL-AD(2004)012-e Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe adopted by the Venice Commission at its 58th Plenary Session.* Retrieved from Venice Commission, Cuoncil of Europe: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e, Aksesuar 02 gusht 2022.

konfirmimin e votës së tyre dhe ta korrigjojnë atë nëse është e nevojshme, duke respektuar votën e fshehtë. Gjithashut ky udhëzim parashikon shetet anëtare duhet të vendosin sanksione për çdo shkelje e të drejtës së fshehtë të votës[18].

Komisioni i Venecias në këtë raport është shprehur për nevojën e vendosjes së disa masave paraprake për të minimizuar rrezikun e mashtrimit, megjithëse metodat mekanike dhe elektronike të votimit paraqesin avantazhe të qarta kur zhvillohen disa zgjedhje në të njëjtën kohë, duke i mundësuar votuesit të kontrollojë votën e tij/saj menjëherë pas dhënies së saj. Kjo formë votimi duhet të pranohet vetëm nëse është e sigurt dhe e besueshme. Në veçanti, zgjedhësi duhet të jetë në gjendje të marrë konfirmimin votën e tij dhe, nëse është e nevojshme, korrigjojë atë pa cenuar në asnjë mënyrë fshehtësinë e votimit. Të gjitha metodat e përdorura duhet të mundësojnë garantimin e konfidencialitetit të fletëvotimit. Metodat e votimit elektronik janë "të sigurta" nëse sistemi mund të përballojë sulmin e qëllimshëm; ato janë "të besueshme" nëse mund të funksionojnë vetë, pavarësisht nga ndonjë mangësi në harduer ose softuer[19].

Në vitin 2014, kur u bë e qartë se pas dhjetë vitesh kishte nevojë për përditësimin e Rekomandimit të vitit (2004)11, u krijua Komiteti Ad Hoc i Ekspertëve për Standardet Ligjore, Operacionale dhe Teknike për Votimin elektronik, i cili përbëhej nga përfaqësues të emëruar nga Shtetet anëtare dhe organizatat me përvojë dhe njohuri të specializuara për votim elektronik. Këtij Komiteti ad hoc iu dha mandati për të rishikuar standardet dhe për të përgatitur një rekomandim të ri në dritën e zhvillimeve të reja në fushën e teknologjive të reja dhe zgjedhjeve[20]. Ky është i vetmi instrument ndërkombëtar që ofron udhëzime se si të përkthehet parimet e trashëgimisë zgjedhore evropiane në kërkesat për sistemet e votimit elektronik. Parimet përfshijnë votën universale, të barabartë, të lirë, të fshehtë dhe të drejtpërdrejtë, organizimin e zgjedhjeve në intervale të rregullta, respektimin e të drejtave themelore, nivelet rregullatore dhe stabilitetin e ligjit zgjedhor dhe garancitë procedurale.

18 Po aty.

19 Venice Commission . (2004, March 12-13). *CDL-AD(2004)012-e Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe adopted by the Venice Commission at its 58th Plenary Session.* Retrieved from Venice Commission, Cuoncil of Europe: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e, Fq. 12, Aksesuar 02 gusht 2022.

20 David Yeregui, Marcos Del Blanco, David Duenas-Cid, Hector Alaiz Moreton. (2020). E-Voting Systems Evaluation based on the Cuncil of Europe Recommandations: nVotes. In M. V.-C. Robert Krimmer, *Electronic Voting 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Proceedings* (pp. 147-167), Fq. 154. Bregenz: Springer

4. Kuadri Ligjor për krimin kibernetik

Instrumentet ligjore që trajtojnë teknologjitë dixhitale janë shumë të rëndësishme edhe pse nuk kanë të bëjnë në mënyrë specifike me zgjedhjet. Megjithëse ka patur vazhdimisht përpjekje dypalëshe dhe shumëpalëshe ndërmjet shteteve, për të luftuar krimin kibernetik, Bashkimi Evropian mbetet në krye të krijimit të një kuadri për krimin kibernetik. Ndër këto përpjekje të Bashkimit Evropian dalin në pah Komunikata e Komisionit për Këshillin e Evropës, Parlamentit Evropian, Komitetit Ekonomik dhe Social dhe Komitetit të Rajoneve për krijimin e një shoqërie informacioni më të sigurt duke përmirësuar sigurinë e infrastrukturës së informacionit dhe duke luftuar krimin e lidhur me kompjuterin[21].

Këshilli i Evropës ka qënë nga institucioni i parë që duke shkuar përtej Bashkimit Evropian ka ftuar edhe shtetet joanëtare për të hartuar dhe përgatitur një instrumenti ligjërisht të detyrueshëm bazuar në rekomandimet e mëparshme të Këshillit të Evropës për luftën ndaj krimit kibernetik. Kështu, si rezultat i një pune intensive 4-vjeçare nga një komision ekspertësh, të cilit Komiteti i Ministrave i besoi përgatitjen e këtij dokumenti për krimin kompjuterik duke përfshirë dispozita thelbësore të ligjit penal dhe instrumente procedurale penale të lidhura me teknologjinë e informacionit[22]. Konventa e Këshillit të Evropës për krimin kibernetik që njihet ndryshe si Konventa e Budapestit shërben si një udhëzues për çdo vend që zhvillon legjislacion kombëtar gjithëpërfshirës kundër krimit kibernetik dhe shërben si kornizë për bashkëpunimin ndërkombëtar ndërmjet shteteve palë në këtë Konventë[23]për vetë faktin se paraqet instrumentet për të përmirësuar bashkëpunimin ndërkombëtar.

Konventa e Budapestit është një dokument në fushën penale që u siguron shteteve (i) kriminalizimin e një liste sulmesh kundër dhe me anë të kompjuterëve; (ii) mjetet e ligjit procedural për ta bërë hetimin e krimit kibernetik dhe sigurimin e provave elektronike në lidhje me çdo krim më efektiv dhe subjekt i mbrojtjeve të sundimit të ligjit; dhe (iii) bashkëpunimi

21 European Commission. (2001, January 26). *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Compu*. Retrieved from Communication of the European Commission 52000DC0890 /* COM/2000/0890 final */: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52000DC0890&from=EN. Aksesuar 05 gusht 2022.

22 Council of Europe. (2001, November 23). *Convention on Cybercrime.* Retrieved from European Treaties Series - - No. 185: https://rm.coe.int/1680081561, Aksesuar 05 gusht 2022.

23 Po aty.

ndërkombëtar policor dhe gjyqësor për krimin kibernetik dhe provat elektronike.

Objektivat kryesore të Konventës ishin: të përcaktojë përkufizime të përbashkëta për disa vepra penale në mënyrë që legjislacioni të mund të harmonizohet në nivel kombëtar; të përcaktojë rregullat e përbashkëta për kompetencat hetuese që i përshtaten mjedisit të teknologjisë së informacionit; të përcaktojnë si llojet tradicionale ashtu edhe ato të reja të bashkëpunimit ndërkombëtar në mënyrë që vendet të mund të bashkëpunojnë me shpejtësi në hetimet dhe ndjekjet e tyre, p.sh. duke përdorur një rrjet kontaktesh të përhershme[24]. Nër të tjëra, Konventa përfshin dispozita të orientuara drejt luftimit të terrorizmit, shfrytëzimit seksual të fëmijëve, krimit të organizuar, shkeljes së të drejtave të autorit, hakimit dhe mashtrimit në internet[25].

Pjesa e parë e Konventës parashikon veprat penale dhe parashtrojnë përkufizime të përbashkëta, të cilat do të eliminonin problemet e kriminalitetit të dyfishtë. Këto nëntë vepra penale, shumë prej të cilave janë përcaktuar tashmë në rekomandimin e vitit 1989 për krimin e lidhur me kompjuterin, ndahen në katër kategori: vepra kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave ose sistemeve kompjuterike; shkeljet e lidhura me kompjuterin; vepra penale të lidhura me përmbajtjen; dhe veprat që përfshijnë shkeljen e pronësisë intelektuale dhe të drejtave të lidhura me to[26]. Pra në këtë pjesë parashikohen të gjitha ato vepra objektivi kryesor i të cilave është sistemi ose të dhënat kompjuterike, prandaj natyra e tyre e dënueshme është e lidhur ngushtë me mjedisin kompjuterik në të cilin ato zhvillohen.

Konventa për krimin kibernetik penalizon disa lloje sjelljesh, përkatësisht krimet e mundshme të drejtuara në zgjedhje. Kompetencat e tij procedurale dhe dispozitat e ndihmës së ndërsjellë juridike janë të rëndësishme kur hetohen dhe procedohen kundër ndërhyrjeve në zgjedhje.

Në ditët e sotme, ajo mbetet marrëveshja ndërkombëtare më e rëndësishme për krimin kibernetik dhe provat elektronike. Akoma dhe më tepër shtete bëhen pjesë e kësaj konvente, ndërkohë që cilësia e zbatimit dhe niveli i bashkëpunimit ndërmjet Palëve vazhdojnë të përmirësohen. Formula e suksesit është një "trekëndësh dinamik"; Konventa e Budapestit plotësohet

24 Nancy E.Marion. (2010, January - July). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation . *International Journal of Cyber Criminology , Vol 4 Issue 1&2*, pp. 699-712. Fq. 701.

25 Po aty.

26 Ian Walden. (2004, January). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, vol. 12*, pp. 321-336. Fq. 331.

nga një mekanizëm efektiv përcjellës dhe nga programet e ngritjes së kapaciteteve, të cilat kthehen në Komitet, duke kontribuar në evoluimin e Konventës.

Komiteti i Konventës për krimin kibernetik, që përfaqëson Palët në Konventën e Budapestit për krimin kibernetik, ka miratuar një shënim udhëzues për të lehtësuar veprimet e drejtësisë penale kundër ndërhyrjeve në zgjedhje duke përdorur kompjuterë. Ndërhyrja në zgjedhje përmes aktiviteteve kibernetike keqdashëse kundër kompjuterëve dhe të dhënave të përdorura në zgjedhje dhe fushata zgjedhore minon zgjedhjet e lira, të ndershme dhe të pastra dhe besimin në demokraci dhe është një kërcënim në rritje dhe shpesh shoqërohet me fushata dezinformuese siç janë përjetuar veçanërisht që nga viti 2016[27].

Palët në Konventën e Budapestit për krimin kibernetik bien dakord se duhen ndërmarrë përpjekje më të mëdha për të ndjekur penalisht një ndërhyrje të tillë kur ajo përbën një vepër penale: "një përgjigje efektive e drejtësisë penale mund të pengojë ndërhyrjen në zgjedhje dhe të sigurojë elektoratin në lidhje me përdorimin e informacionit dhe komunikimit. teknologjitë në zgjedhje". Prandaj, Udhëzimi tregon se cilat mjete të Konventës së Budapestit janë në dispozicion për të hetuar dhe ndjekur penalisht këto aspekte të ndërhyrjes në zgjedhje. Ky Udhëzim nënvizon edhe një herë se Konventa e Budapestit e Këshillit të Evropës mbetet marrëveshja ndërkombëtare më e rëndësishme për krimin kibernetik dhe provat elektronike për të adresuar kërcënimet aktuale ndaj të drejtave të njeriut, demokracisë dhe sundimit të ligjit në hapësirën kibernetike[28].

Një nga instrumentet e tjerë ndërkombëtarë është edhe Konventa e Modernizuar e Këshillit të Evropës për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale (Konventa 108+)[29], e lidhur me instrumenti referues i BE-së, Rregullorja (BE) 2016/679 e

27 Sandeep Mittal, Priyanka Sharma. (2017, May-June). A Review of International Legal Framework to Combat Cybercrime. *International Journal of Advanced Research in Computer Science, Volume 8, No. 5,* , pp. 1372- 1374.Fq. 1372.

28 Council of Europe. (2019, July 10). *Tools for combatting malicious cyber interference with elections*. Retrieved from Council of Europe News: https://www.coe.int/en/web/portal/home/-/asset_publisher/CWAECqDHgT3y/content/tools-for-combatting-malicious-cyber-interference-with-elections?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fportal%2Fhome%3Fp_p_id%3D101_INSTANCE_CWAE, Aksesuar 09 gusht 2022.

29 Council of Europe. (2018, May 18). *Convention 108 and Protocols: Convention for the protection of individuals with regard to the processing of personal data.* Retrieved from Council of Europe Convention 108+: https://www.coe.int/en/web/data-protection/convention108-and-protocol, Aksesuar 09 gusht 2022.

Parlamentit Evropian[30] dhe Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave e Këshillit Evropian, u bënë drejtpërdrejt e zbatueshme në të gjithë Bashkimin Evropian më 25 maj 2018. Sipas Këshillit Evropian, ajo i ofron Bashkimit Evropian mjetet e nevojshme për të adresuar rastet e përdorimit të paligjshëm të të dhënave personale në kontekstin elektoral. Sipas Këshillit shumica e të dhënave të përdorura në zgjedhje janë të dhëna të kualifikuara, përpunimi i të cilave mund të lejohet vetëm nëse masat e duhura mbrojtëse janë të parashikuara në ligj. Kjo do të thotë që mbrojtja online e të dhënave zgjedhore duhet të mbulohet në rregulloret specifike për zgjedhjet, të cilat duhet të jenë më të rrepta se instrumentet e mbrojtjes së të dhënave[31].

Në pesëvjeçarin e fundit është duke u shfaqur në Evropë një legjislacioni transnacional mbikombëtar për sigurinë kibernetike., Direktiva për sigurinë e rrjeteve dhe sistemeve të informacionit e miratuar nga Parlamenti Evropian në korrik 2016 është pjesa e parë e legjislacionit në mbarë BE-në për sigurinë kibernetike[32]. Kjo Direktive siguron masa ligjore për të rritur nivelin e përgjithshëm të sigurisë kibernetike në BE duke kërkuar që shtetet anëtare të pajisen siç duhet, duke krijuar një grup bashkëpunimi për të mbështetur dhe lehtësuar bashkëpunimin strategjik për incidentet e sigurisë kibernetike dhe shkëmbimin e informacionit rreth rreziqeve dhe promovimin e kulturës së sigurinë në të gjithë sektorët që janë jetik për ekonominë dhe shoqërinë[33]. Pas Direktivës, në vitin 2019 u miratua një Akt i BE-së për sigurinë kibernetike, i cili prezanton, për herë të parë, një kornizë certifikimi të sigurisë kibernetike në mbarë BE-në për produktet, shërbimet dhe proceset e teknologjisë së informacionit[34].

30 European Parliament, Council of Europe. (2016, July 6). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved from Official Journal of the European Union-European Union Agency for Cybersecurity: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN, Aksesuar 11 gusht 2022.

31 European Union. (2020, January). *General Data Protection Regulation (GDPR)*. Retrieved from Complete guide to GDPR compliance: https://gdpr.eu/tag/gdpr/, Aksesuar 11 gusht 2022.

32 European Parliament, Council of Europe. (2016, July 6). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved from Official Journal of the European Union-European Union Agency for Cybersecurity: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN, Aksesuar 11 gusht 2022.

33 ENISA. (2020, December 11). *The EU Cybersecurity strategy* . Retrieved from European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/nis-directive, Aksesuar 13 gusht 2022.

34 European Parliament, Council of Europe. (2019, June 7). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52.* Retrieved from Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN, Aksesuar 13 gusht 2022.

Në lidhje me procesin e zgjedhjeve, theksi është vënë prej vitit 2016 në sigurinë kibernetike të zgjidhjeve dixhitale të përdorura dhe aplikimin konkret të instrumenteve ndërkombëtare për mbrojtjen e të dhënave apo sigurinë kibernetike të të gjithë procesit të zgjedhjeve. Komisioni Evropian ka nxjerrë udhëzime për zbatimin e ligjit të Bashkimit Evropian për mbrojtjen e të dhënave në kontekstin zgjedhor[35]. Puna në nivel të BE-së për sigurinë kibernetike të teknologjisë zgjedhore rezultoi në një Përmbledhje mbi Sigurinë Kibernetike të Teknologjisë Zgjedhore që synon shkëmbimin e përvojave dhe duke ofruar udhëzime, si dhe një pasqyrë të mjeteve, teknikave dhe protokolleve për zbulimin, parandalimin dhe zbutjen e kërcënimeve kibernetike[36] (ENISA, 2018).

5. Konkluzione

Ndërsa hapësira kibernetike po evoluon me shpejtësi me ardhjen e teknologjive të reja, krimi kibernetik po merr dimensione të reja, për këtë siguria kibernetike zgjedhore është një angazhim afatgjatë që kërkon zbatim gjatë gjithë ciklit zgjedhor. Teknologjitë e përdorura në zgjedhje mund të ndryshojnë me çdo cikël elektoral, dhe po kështu ndryshojnë edhe kundërshtarët dhe mjetet e tyre. Prandaj, siguria gjithëpërfshirëse elektorale kibernetike kërkon angazhim dhe burime të vazhdueshme. Edhe vendet që përdorin vetëm teknologji të kufizuar në zgjedhje përballen me rreziqe kibernetike ndaj integritetit zgjedhor që kërkojnë konsideratë serioze.

Konventa për krimin kibernetik është, një përpjekje e madhe për të identifikuar çështjet dhe për t'i dhënë zgjidhje boshllëqeve ekzistuese ligjore dhe procedurale në luftimin e krimit kibernetik. Megjith punën e madhe të Këshillit të Evropës dhe BE-së përsëri nuk është i mjaftueshëm I gjithë kuadri ligjor I miratur si dhe instrumentat ndërkombëtarë në funksion të ruajtjes së zgjedhjeve në sistemet elektronike. Në mënyë që të arrihet suksesi në këtë fushë duhet të arrihet një bashkëpunim në rang ndërkombëtar dhe jo rajonal evropian. Gjithashtu shtetet duhet të miratojnë legjislacion të posaçëm që

35 European Commission. (2018, September 12). *Guidance Document COM(2018) 638 final, Commission guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0638&from=EN, Aksesuar 13 gusht 2022.

36 ENISA. (2018, July). *Compendium on Cyber Security of Election Technology.* Retrieved from CG Publication 03/2018, Directive (EU) 2016/1148: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf, Aksesuar 13 gusht 2022.

parashikon si vepër penale spcifike dhe ndërhyrjen në zgjedhje nëpërmjet sistemeve elektronike, e përforcuar kjo qoftë në legjislacionin zgjedhor ashtu edhe në atë penal.

Bibliography

Committee of Ministers, Council of Europe. (2017, June 14). *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting.* Retrieved from Committee of Ministers, CM/Rec(2017)5 : https://rm.coe.int/0900001680726f6f

Alexander H. Trechsel, Vasyl Kucherenko, Frederico Silva, Urs Gasser. (2016, May). *Potential and Challenges of e-voting in the European Union.* Retrieved from European Parliament, Directorate-General for Internal Policies, Policy Department, Citizen's Rights and Constitutional Affairs: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf

Ben Goldsmith, Holly Ruthrauff. (n.d.). *Case Study Report on Electronic Voting in the Netherlands.* Retrieved from NDI, Implementing and Overseeing Electronic Voting and Counting Technologies: https://www.ndi.org/sites/default/files/5_Netherlands.pdf

Caarls, S. (2010, November). *E-voting Handbook: Key Steps for Introducing E-voting.* Retrieved from Council of: https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf

Committee of Ministers, Council of Europe. (2004, September 30). *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.* Retrieved from Committee of Ministers, Rec(2004)11: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp

Council of Europe. (2001, November 23). *Convention on Cybercrime.* Retrieved from European Treaties Series - - No. 185: https://rm.coe.int/1680081561

Council of Europe. (2018, May 18). *Convention 108 and Protocols: Convention for the protection of individuals with regard to the processing of personal data.* Retrieved from Council of Europe Convention 108+: https://

www.coe.int/en/web/data-protection/convention108-and-protocol

Council of Europe. (2019, July 10). *Tools for combatting malicious cyber interference with elections*. Retrieved from Council of Europe News: https://www.coe.int/en/web/portal/home/-/asset_publisher/CWAECqDHgT3y/content/tools-for-combatting-malicious-cyber-interference-with-elections?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fportal%2Fhome%3Fp_p_id%3D101_INSTANCE_CWAE

David Yeregui, Marcos Del Blanco, David Duenas-Cid, Hector Alaiz Moreton. (2020). E-Voting Systems Evaluation based on the Cuncil of Europe Recommandations: nVotes. In M. V.-C. Robert Krimmer, *Electronic Voting 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Proceedings* (pp. 147-167). Bregenz: Springer.

ENISA. (2018, July). *Compendium on Cyber Security of Election Technology.* Retrieved from CG Publication 03/2018, Directive (EU) 2016/1148: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

ENISA. (2020, December 11). *The EU Cybersecurity strategy* . Retrieved from European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/nis-directive

European Commission. (2001, January 26). *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Compu*. Retrieved from Communication of the European Commission 52000DC0890 /* COM/2000/0890 final */: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52000DC0890&from=EN

European Commission. (2018, September 12). *Guidance Document COM(2018) 638 final, Commission guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0638&from=EN

European Parliament, Council of Europe. (2016, July 6). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved from Official Journal of the European Union-European Union

Agency for Cybersecurity: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

European Parliament, Council of Europe. (2016, April 17). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.* Retrieved from Official Journal of the European Union, EUR-Lex: http://data.europa.eu/eli/reg/2016/679/oj

European Parliament, Council of Europe. (2019, June 7). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52.* Retrieved from Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

European Union. (2020, January). *General Data Protection Regulation (GDPR)*. Retrieved from Complete guide to GDPR compliance: https://gdpr.eu/tag/gdpr/

International IDEA. (2011). *Introducing Electronic Voting: Essential Considerations* . Stockholm: INTERNATIONAL IDEA.

Marion, N. E. (2010, January - July). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation . *International Journal of Cyber Criminology , Vol 4 Issue 1&2*, pp. 699-712.

NDI. (2013, December 17). *The Constitutionality of Electronic Voting in Germany*. Retrieved from National Democratic Institute- Implementing and Overseeing Electronic Voting and Counting Projects: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany

Sandeep Mittal, Priyanka Sharma. (2017, May-June). A Review of International Legal Framework to Combat Cybercrime. *International Journal of Advanced Research in Computer Science, Volume 8, No. 5,* , pp. 1372- 1374.

United Nations. (1966, December 16). *International Covenant on Civil and Political Rights*. Retrieved from UNHCR, Human Rights Instruments: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Venice Commission . (2004, March 12-13). *CDL-AD(2004)012-e*

Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe adopted by the Venice Commission at its 58th Plenary Session. Retrieved from Venice Commission, Cuoncil of Europe: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e

Vollan, K. (2006). Voting in uncontrolled environment and the secrecy of the vote. *Electronic Voting 2006, 2nd International Workshop, Co-organized by Council of Europe* (pp. 155-169). Bregenz, Austria: Council of Europe.

Walden, I. (2004, January). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, vol. 12*, pp. 321-336.

PROTECTION OF VICTIMS FROM CRIMINAL OFFENSES CAUSED BY TECHNOLOGICAL DEVELOPMENTS

PROF.ASSOC. DR. LIRIME CUKAJ

Faculty of Law University of Tirana

lilicukaj@yahoo.it

ADV. DENISA LAÇI

Agency of Agriculture and Rural Development

lacidenisa@gmail.com

Abstract

The development of technology has brought about its use to commit a criminal offense, but so has been used to detectthe offenses.

In this paper, a particular focus is given in how is foreseen in the criminal and procedural legislation, protection of victims of criminal offenses committed through technology.

The subject of this paper focuses on the protection that the Albanian lawmaker has given to the victims of this category in protecting and insuring an effective access to the justice system.

The interventions of the lawmaker since 2016 have aimed on guaranteeing an effective access of the victim of the criminal offense at the criminal proceeding's stages, through informing about the state of the proceedings, the active role in obtaining evidence, not only through the requests addressed to the prosecutor, but also by taking the evidence itself, when she is an

accusatory victim.

This paper attempts to address whether the criminal procedural system has guaranteed effective ways to assist the victim, the accusatory victim, in gathering evidence when she is injured by the criminal offense in the field of technology. The Albanian system foresees a list of rights for victims, but the matter consists of how much cybercrime infrastructure allows them to exercise these rights, there remains a need for further discussion and normally for legal improvements in Albanian procedural system.

Keywords:*cyber-crime, organized crime, falsification, sabotage, secret provision, strategy, pornography, theft, fraud, criminal offences.*

Author:

Lirime Cukaj,was born on 17 February 1975. Graduated in high- school "Zyrhana Xhako Balabam, Permet at 1988-1992. Studies and graduated in Nursing Faculty, University "Fans S. Noli", Korce at 1994-1998. Follows up studies at Faculty of Law University of Tirana at 2001-2005. Postgraduate studies (second level MASTER) at 2006-2008. From 2009 to 2014, doctoral studies at the Criminal Department, Faculty of Law, University of Tirana. Upon completion of the studies, I was awarded the doctoral degree. 2016, Associate Professor. Teaches criminal law and criminal procedural law at Faculty of Law University of Tirana. With an experience of 7 years, lawyer in criminal, civil and public law from 2014. Author of several scientific papers published in national and international journals.

Denisa Laçi,was born on 30.10.1995, Followed up studies at Faculty of Law University of Tirana at 2014-2017. Postgraduate studies Scientific Penal Master at 2017-2019. In 2020 follows up studies at Advocacy school. Since 2019 experience working in public administration in different positions. Author and co-author of several scientific papers regarding different topics limited not only on criminal law, published in national and international journals.

Hyrje

Viktima e veprës penale, me ndryshimet që ka pësuar Kodi i Proçedurës Penale, është një subjekt me rol më aktiv gjatë këtij proçedimi[1], Megjithatë ende në kod ne gjejmë ndarjen klasike të viktimës në:

- Viktima që akuzon,[2] në këtë rast palën akzuese e bënë viktima e cila inicion nëpërmjet kallëzimit ndjekjen penale të autorëve të disa prej veprave penale të listuara në nenin 59 drejtpërsëdrejti në gjykatë.
- Viktima që bën ankim, kundrejt vendimarrjes së organeve të drejtësisë.
- Viktima që nuk bën as ankim, as nuk akuzon, por ushtrimi i ndjkes penale ndiqet kryesisht nga prokuroria si organ i akuzës.

Zhvillimet e teknologjisë, kanë sjellë përdorimin e këtij zhvillimi me efikasitet në luftën kundër krimit, por njëkohësisht teknologjia ka shërbyer edhe për të kryer vepra penale.Në këtë punim do të ndalemi tek veprat

1 Për më shumë shiko nenin 58 të K.Pr. Penale të ndryhsuar Neni 58
Të drejtat e viktimës së veprës penale
(Shtuar pika 3 me ligjin nr.8813, datë 13.6.2002 dhe ndryshuar me ligjin nr. 35/2017, datë 30.3.2017)
1. Viktima e veprës penale ka të drejtë: a) të kërkojë ndjekjen penale të fajtorit; b) të përfitojë kujdes mjekësor, ndihmë psikologjike, këshillim dhe shërbime të tjera të ofruara nga autoritetet, organizatat ose institucionet përgjegjëse për ndihmën ndaj viktimave të veprës penale; c) të komunikojë në gjuhën e saj dhe të ndihmohet nga një përkthyes, interpretues i gjuhës së shenjave ose lehtësues i komunikimit për personat me aftësi të kufizuar në të folur dhe në të dëgjuar; ç) të zgjedhë mbrojtës dhe, kur është rasti, të përfitojë ndihmë juridike falas, sipas Legjislacionit në fuqi; d) të kërkojë në çdo kohë informacion për gjendjen e procedimit, si dhe të njihet me aktet e provat, pa cenuar parimin e sekretit hetimor; dh) të kërkojë marrjen e provave, si dhe të parashtrojë kërkesa të tjera përpara organit procedues; e) të informohet për arrestimin e të akuzuarit dhe lirimin e tij, në kushtet e caktuara në këtë Kod; ë) të njoftohet për mosfillimin e procedimit, pushimin e çështjes, fillimin dhe përfundimin e gjykimit; f) të bëjë ankim në gjykatë kundër vendimit të prokurorit për të mos filluar procedimin dhe vendimit të prokurorit ose gjyqtarit të seancës paraprake për të pushuar akuzën ose çështjen; g) të kërkojë shpërblimin e dëmit dhe të pranohet si paditës civil në procesin penal; gj) të përjashtohet, në kushte të caktuara me ligj, nga pagimi i çdo shpenzimi për marrjen e akteve dhe tarife gjyqësore për paraqitjen e kërkesë-padisë që lidhen me statusin e viktimës së veprës penale; h) të thirret në seancën paraprake dhe në seancën e parë gjyqësore; i) të dëgjohet nga gjykata, edhe kur asnjëra nga palët nuk ka kërkuar thirrjen e saj si dëshmitar; j) të ushtrojë të drejta të tjera të parashikuara nga ky Kod.
2. Organi procedues njofton menjëherë viktimën për të drejtat e përmendura në paragrafin 1, të këtij neni, dhe mban procesverbal për njoftimin e tyre.
3. Viktima që nuk ka zotësi për të vepruar i ushtron të drejtat e saj nëpërmjet përfaqësuesit ligjor ose kujdestarit të tij, përveçse kur kjo nuk është në interesin e viktimës. Kur vëren papajtueshmëri mes interesave të viktimës dhe atyre të përfaqësuesit ligjor ose kujdestarit, gjykata cakton një kujdestar të posaçëm, në përputhje me dispozitat e Kodit të Familjes.
4. Trashëgimtarët e viktimës kanë të drejtat e parashikuara në shkronjat "a", "e", "ë", "f", "g" dhe "j", të paragrafit 1, të këtij neni. Nëse trashëgimtari i viktimës është i mitur, ai përfaqësohet nga kujdestari ligjor.

2 Kodi i Procedures Penale neni 59

penale që drejtohen ndaj viktimës, ku mjeti për të kryer veprën penale, është përdorimi i teknologjisë dhe internetit.Por njëkohësisht do të trajtojmë edhe mjetet që ka në dispozicion viktima e veprës penale, në rastet kur ajo është viktima që akuzon dhe shkon drepërdrejtë në gjykatë. Në këto raste ajo ka barrën e provës për të provuar akuzën që do të ngrej para gjykatës.

Në këtë trajtim do të shohim problematikat që ka në praktikë, viktima akuzuese, në proçesin e të provuarit, duke analizuar mundësitë ligjore për të aksesuar drejtësinë në këto raste, problematikat e praktikës dhe duke konkluaduar në rekomandime mbi mënyrën e zgjidhjes së këtyre problemeve.

METODOLOGJIA

Në realizimin e këtij artikulli, fokusi i të cilit është vëzhgimi dhe krahasimi i dispozitave penale dhe proceduriale në lidhje me viktimën akuzuese për vepra penale që lidhen me teknologjinë dhe internetin, në fushën që ata trajtojnë, kemi aplikuar një sërë metodash:

- **Metoda Analitike** – Vëmendje e veçantë i do ti kushtohet analizimit të dispozitave që sanksionojnë veprat penale të cilat kryhen nëpërmjet teknologjisë.

- **Metoda krahasimore** – I gjithë qëllimi i këtij punimi është krahasimi i këtyre rregullimeve ligjore me ndryshimet e aplikuara në këtë mënyrë mund të kuptohet evoluimi i legjislacionit në aspektin e përmirësimit të pozitës së viktimave të veprave penale në përgjithësi dhe viktimave të krimit teknologjik në veçanti.

1. Viktima akuzuese

Viktima akuzuese është subjekt, i cili është i dëmtuar nga vepra penale të parashikuara nga nenin 59 i K.Pr.Penale[3], vepra penale këto qëkanë një rrezikshmëri të ulët dhe që prekin interesat ngushtësisht personale, pra vetëm

3 Neni 59 Viktima akuzuese "*1. Ai që është dëmtuar nga veprat penale të parashikuara nga nenet 90, 91, 92, 112 paragrafi i parë, 119,119/b, 120, 121, 122, 43 125, 127, dhe 254 të Kodit Penal ka të drejtë të paraqesë kërkesë në gjykatë dhe të marrë pjesë në gjykim si palë për të vërtetuar akuzën dhe për të kërkuar shpërblimin e dëmit. 2. Prokurori merr pjesë në gjykimin e këtyre çështjeve dhe, sipas rastit, kërkon dënimin e të pandehurit ose pafajësinë e tij. 3. Nëse viktima akuzues ose mbrojtësi i caktuar prej tij nuk paraqitet në seancë pa shkaqe të arsyeshme, gjykata vendos pushimin e gjykimit. 4. Viktima akuzuese që nuk ka zotësi për të vepruar i ushtron të drejtat që i janë njohur me ligj nëpërmjet përfaqësuesit ligjor. 5. Kur disa viktima të së njëjtës çështje paraqesin kërkesë në gjykatë, sipas nenit 59, të këtij Kodi, kërkesat e tyre bashkohen në një gjykim të vetëm".*

të personit të dëmtuar nga vepra penale dhe që ndjekja penale nuk ushtrohet dot kryesisht nga prokuroria, pasi nuk ka njëinteres publik të cënuar.Në këto raste nuk kemi një akuzë publike, por kemi një akuzë private, të ngritur nga vet viktima e veprës penale.

Ndër këto vepra penale për të cilat viktima e veprës penale shkon drejtpërdrejtë në gjykatë dhe ka barrën e provës është edhe vepra penale e parashikuar nga neni neni 119/b

Neni 119/b i Kodit Penal "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik".

Fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

Për këtë kundravajtje penale si të gjitha kundravajtjet e tjera penale, viktima bën kërkesë të drejtpërdrejtë në gjykatë dhe ka barrën e provës për të provuar akuzën private ndaj autorit të dyshuar, pra personit të akuzuar, për kryerjen e kësaj vepre penale.

Neni 121

Ndërhyrje të padrejta në jetën private

Vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimi ose regjistrimi i fjalëve, fiksimi ose regjistrimi figurave, si dhe ruajtja për publikim i të dhënave që ekspozojnë një aspekt të jetës private të personit, pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

Shpërndarja, ofrimi për publikim apo publikimi me çdo mjet ose formë të komunikimit publik apo mënyrë tjetër i të dhënave të marra në mënyrën e përcaktuar në paragrafin e parë të këtij neni, dënohet me burgim deri në tre vjet.

Po kjo vepër, kur kryhet ndaj personave të mitur, dënohet me burgim nga një deri në tre vjet.

Kur vepra penale kryhet nëpërmjet shfrytëzimit të funksionit shtetëror ose shërbimit publik apo nga personi që disponon këto të dhëna për shkak të detyrës shtetërore apo shërbimit publik, dënohet me burgim nga një deri në tre vjet.

Praktika ka treguar një mungesë të theksuar të sistemeve të shqipërisë në

kuadër të ruajtjes së të dhënave të individëve, por ajo cka është më alarmante është mungesa e masave që duket qartazi që nuk po merren nga institucionet kompetente dhe që po pasohen me sulme të njëpasnjëshme kibernetike të sistemeve shtetërore të cilëve u janë besuar të dhënat e qytetarëve të këtij vendi.

Dëshmi e qartë e këtyre problemeve janë publikimi si fillim i emrave të qytetarëve me numrat e ID dhe numrat e telefonit duke u ndarë me bindje politike. Duke u pasuar më pas me publikimin e vendeve të punës dhe pagën mujore të qytetarëve, një shkelje akoma më flagrante që tregonte aksesimin në sistemin tatimor shtetëror.

Përgjegjësia e vetëme që u mbajt ishte dorëheqje të disa prej personave përgjegjës në institucione, veprime fictive që nuk tregojnë forcën vepruese të një shteti në luftimin dhe reagimin e duhur ndaj situatave të tilla. Autorët e vërtet deri më tani nuk janë zbuluar dhe nuk dihet nëse kemi një veprimtari konkrete të zhvilluar apo që po ndërmerret në kuadër të kësaj situate.

2.Viktima që bën ankim

Një subjekt tjetër, i proçedimit penal, është edhe viktima që bën ankim. Vullneti i këtij subjekti i shprehur npm mjetit procedurial, ankimit, është kusht që procedimi penale të fillojë, të vazhdojë apo të përfundojë, pasi pa vullnetin e viktimës që bën ankim nuk ka procedim. Ky subjekt është parashikuar në nenin 284 të K.Pr.Penale[4]. Nga një vëzhgim që i bëhet kësaj dispozite, vërehet se nuk kemi të parashikuar asnjë vepër penale, e cila të kryhet npm teknologjisë së informacionit apo përdorimit të internetit,pasi veprat penale e parashikuara në këtë dispozitë janë, kanosja, plagosja e lehtë me dashje, marrëdhëniet seksuale me dhumë me të rrituara, marrëdhëniet seksuale osehomoseksulale me persona në gjini ose nënkujdestari, shtrëngimi ose pengimi për të bashkëjetuar ose për të zgjidhur martesë, botimi i veprës se tjetrit në emerin e vet, shkeje e të drejtave të autorit, goditje ndaj pjestarit të familjes që kryen detyrë shtetërore, shkelja e paprekshmërisë banesës,

4 Neni 284 Ankimi1. Për veprat penale të parashikuara nga nenet 84, 89, 102 paragrafi i parë, 105, 106, 130, 148,149, 243, 254, 264, 275, 290 paragrafi i parë dhe 318 të Kodit Penal, ndjekja penale mund të fillojë vetëm me ankimin e viktimës, i cili mund ta tërheqë atë në çdo fazë të procedimit.2. Ankimi bëhet nga viktima te prokurori ose në policinë gjyqësore me anën e një deklarate, nëtë cilën personalisht ose nëpërmjet përfaqësuesit të posaçëm, shfaqet vullneti që të procedohet nëlidhje me një fakt të parashikuar nga ligji si vepër penale.3. Kur ankimi bëhet me gojë procesverbali që mbahet për këtë qëllim nënshkruhet nga ankuesiose përfaqësuesi i tij.4. Ai që merr ankimin sigurohet për identitetin e ankuesit dhe i dërgon aktet prokurorit.5. Për rastet e parashikuara nga neni 59, ankimi bëhet në gjykatë nga viktima akuzuese.

detyrimi për të marrë ose jo pjesë në grevë, keqpërdorimi me dashje i thirrjeve telefonike, shkelja e rregullave të qarkullimit rrugor, me pasojë dëmtimine lehtë të disa personave dhe fyerja e gjyqtarit, prokurorit, avokatit.

Pra ligjëvënësi për vepra penale që mund të kryhen nëpërmejt teknologjisë dhe informacionit, nuk ka parashikuar asnjë vepër penale të re, por i ka qëndruar traditës së mëparshme duke lëne ato vepra penale që kanë qenë, duke shtuar në 2017, vetëm veprën penale të shkeljes së rregullave tëqarkullimit rrugor më pasojë dëmtimin e lehtë të disa personave.

3.Viktima që nuk bën kërkesë për gjykim dhe as nuk bën ankim

Përveç viktimës që bën kërkesë për gjykim drejtpërdrejtë në gjykatë dhe viktimës që bën ankim, K.Pr.Penale parashikon edhe viktimën për vepra penale që ndiqet kryesisht.

Në këto raste, organ i akuzës ushtron ndjekjen penale kryesisht pasi ka dëmtim të interesave publike përvec atyre private. Viktima jo vetëm që nuk ka ndonjë rol në ushtrimin e ndjekes penale, por ajo nuk ka as barrën e provës për të provuar ekzistencën e faktit penal dhe të autorit, pasi këto janë atribut i organit të ushtrimit të ndjekjes penale, prokurorisë. Në këto raste është ky organ që ka barrën e provës për të provuar ekzistencën e faktit penal dhe të autorit, me standartin "*tej cdo dyshimi të asryeshëm*". Ajo që vihet re është se ligjëvënësi në këto raste për të hetuar për vepra penale që ndiqen kryesisht dhe që kryehen nëpërmjet teknologjisë ose informacionit, ja ka lënë barrën e provës organit të akuzës, i cili është subjekti që mbledh provat gjatë fazës së hetimit paraprak.

4. Viktima akuzues dhe barra e provës për veprat penale që kryehen nëpërmjet teknologjisë dhe internetit

Viktima akuzuese, ka barrën e provës në procesin penal për të provuar para gjykatës, akuzën penale dhe autorin e veprës penale.Në këtë trajtim do të ndalemi tek barra e provës për veprat penale të kryera nga teknologjia dhe interneti sic janë ato të parashikuara në nenin 119/b dhe 121 të Kodit Penal.

Neni 119/b i Kodit Penal.Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik

Fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën

kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

Për këtë kundravajtje penale si të gjitha kundravajtjet e tjera penale, viktima bën kërkesë të drejtpërdrejtë në gjykatë dhe ka barrën e provës për të provuar akuzën private ndaj autorit të dyshuar, pra personit të akuzuar, për kryerjen e kësaj vepre penale. Ashtu sic përcaktohet në nenin 119/b, kjo vepër penale fyerja me motive racizimi ose ksenofobie, kryhet nëpërmejt sistemit kompjuterik.

Ashtu sic thamë më sipër viktima akuzuese, ka barrën e provës për të provuar konsumimin e kësaj kundravajtje penale. Procesi i të provuarit në këtë kundravajtje penale, konsiston përvec provave të tjera edhe në marrjen e materialeve nga sistemi kompjuterike me përmbajtje racise ose ksenofobike dhe paraqitjen e këtyre materialeve para gjykatës, por marrja e këtyre materialeve, të cilat përmbajnë të dhëna mbi rrethanat dhe faktet e kryerjes së veprës penale nga viktima akuzuese e bën të vështirë marrjen e këtyre materialeve, për shkak se nuk ka njohuritë e posacme teknike për të bërë të mundur marrjen e këtyre të dhënave sepse i mungojnë njohuritë e posacme.

Sipas dispozitave të K.Pr.Penale, nenit 149 dhe 151 janë përcaktuar subjektet që marrin prova që janë opgj, prokuror dhe gjykata.

Sipas këtij rregullimi ligjor, viktima mund ti marrë vet këto të dhena sipas nenit 191 të K.Pr.Penale, në cilësinë e dokumentit që jep të dhëna, ose ti bëj kërkesë gjykatës dhe kjo e fundit të caktojë një ekspertë që ti marr këto të dhëna.

Dsikutimi që lind në këtë rast është se të dhënat e mbledhura nga viktima akuzues nëpëmjet provës, dokument që jep të dhëna, sipas nneit 191, a është një provë e marrë sipas parashikimeve të kodit, në kuptimin e vërtetësisë së kësaj prove, pasi vërtetësia e kësaj prove mund të kundërshtohet nga pala tjetër, pasi mund të ketë ndërhyrje. Në rast kundërshtimi të vërtetesisë së kësaj prove, duhet që të kryhet akt ekspertimi i kësaj prove, për të konkluduar mbi vërtetësinë e saj, duke caktuar një person që ka njohuri të posacme nga sistemet kompjuterike.

Neni 121

Ndërhyrje të padrejta në jetën private

Vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimi ose regjistrimi i fjalëve, fiksimi ose regjistrimi figurave, si dhe ruajtja për publikim i të dhënave që ekspozojnë një aspekt

të jetës private të personit, pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

Shpërndarja, ofrimi për publikim apo publikimi me çdo mjet ose formë të komunikimit publik apo mënyrë tjetër i të dhënave të marra në mënyrën e përcaktuar në paragrafin e parë të këtij neni, dënohet me burgim deri në tre vjet.

Në kundravajtjen tjetër penale, atë të ndërhyrjes në jetën private, parashikohet se kjo k.penale kryehet nëpërmejt vendosjes së aparaturave që përgjojnë, incizojnë, dëgjojnë dhe se këto të dhëna të mbledhura nëpërmejt këtyre pajisjeve mund të përhapen edhe nëpërmejt teknologjisë dhe informacionit dhe shpesh ato përhapen npm mjeteve të tilla, sic janë publikimet nëëeb, apo në aplikacione të ndryshme.

Në këtë kundravajtje penale, procesi i të provuarit, konsiston në sekuestrimin e këtyre rregjistrimeve, filmimeve dhe paraqitjen në gjykatë. I njëjti diskutim mund të lind sërish në lidhje me vërtetësinë e kësaj prove të marrë dhe të sjellë në gjykim nga viktima akuzuese.

5.Provat dhe mjetet e kërkimit provës që përdoren nga viktima akuzuese në procesin e të provuarit.

Viktima akuzuese, referuar barrës së provës, ka detyrimin ligjor, që të marrë dhe tëçojë para gjykatës të gjitha provat dhe mjetet e kërkimit të provës, nga atoo që K.Pr.Penale parashikon nga neni 149 e në vijim. Një nga mjetet e kërkimit të provës që lidhen me veprat penale të kryera nëpërmjet teknologjisëështë edhe sekuetsrimi i të dhënave kompjutërike.

Në nenin 208/a të K.Pr.Penale, parashikohet sekuestrimi i të dhënave kompjuterike, për vepra penale që lidhen me teknologjinë dhe informacionin. Si të gjitha mjetet e kërkimit të provës që kanë tendencën fiziologjike të cënojnë nenin 8 të KEDNJ-së, Kodi i Pr.Penale, parashikon mënyrën si merret këto të dhëna komjuterike[5].

5 Neni 208/a Sekuestrimi i të dhënave kompjuterike
1. Në rastin e procedimeve për krime që lidhen me teknologjinë e informacionit, gjykata, me kërkesën e prokurorit, urdhëron sekuestrimin e të dhënave ose sistemeve kompjuterike. Në këtë vendim gjykata përcakton të drejtën për të hyrë, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimin për kryerjen e veprimeve të mëtejshme apo sigurimin e të dhënave ose të sistemit kompjuterik.
2. Kur ekzistojnë shkaqe të arsyeshme për të menduar se të dhënat e kërkuara kompjuterike janë memorizuar në një sistem tjetër kompjuterik apo në një pjesë të tij dhe këto të dhëna janë në mënyrë të ligjshme të kapshme prej ose janë të disponueshme nga sistemi kompjuterik fillestar, që kontrollohet, gjykata, me kërkesë të prokurorit, urdhëron menjëherë kërkimin ose hyrjen

Sekuestrimi i tëdhënavekompjuterikepër krime që lidhen me teknologjinë e informacionit bëhet me vendim nga gjykata, mekërkesën e prokurorit. Gjykata në këtë vendim urdhëron sekuestrimin e të dhënave ose sistemeve kompjuterike edhe në një system tjetër rrjeti. Ekzekutimi i këtij vendimi bëhet nga prokuroria oseoficeri i policisë gjyqësore. Ata kanë të drejtë që të asistohen nga njëekspert, i cili kanjohuri rreth funksionimit të sistemeve kompjuterike apo të masave të zbatuara për mbrojtjen e tëdhënave kompjuterike në të.

Sekuestrimi i të dhënave komjuterike bëhet me vendim të gjykatës dhe ky vendim ekzekutohet nga prokurori dhe me delegim nga oficeri i policisë gjyqësore.

Ky parashikim është në përputhje me juridiksionin e GJEDNJ-së, e cila në respektim të së drejtës për privatci, përcakton gjykatën si një subjekt plotësisht i pavarur, të urdhërojë dhe të kontrollojë sekuestrimin e të dhënave komjuterike. Sigurisht ky parashikim ligjor është garanci për mbrotjen e të drejtës për jetë private, por duket se nuk i jep shumë akses viktimës së veprës penale. Ashtu sic kemi përmendur më sipër, viktima akuzuese ka barrën e provës për të provuar k.penale të fyerjes 119/b, Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik dhe 121 të Kodit Penal dhe ndërhyrje të padrejta në jetën private, një nga mjetet e kërkimit të provës, qëështë i domosdoshëm në këtë rast është edhe sekuestrimi I të dhënave komjuterike. Por marrja e këtyre të dhënave, kërkon vendim gjykate dhe ekzekutim nga prokuroi, për shkak të rregullimit specific që ka vendosur nenin 208/a i K.Pr.Penale. Marrja e këtyre të dhënave mund të bëhet vetëm në seancë gjyqësore me kërkesë të viktimës akuzuese[6], pasi ky subjek për shkak të rregullimit specific të këtij neni nuk mundet dot ti marrë këto të dhëna nga

---

edhe në këtë sistem kompjuterik.
3. Në zbatim të vendimit të gjykatës, prokuroria ose oficeri i policisë gjyqësore, i deleguar nga prokurori, merr masa:
a) për të ndaluar kryerjen e veprimeve të mëtejshme ose për të siguruar sistemin kompjuterik, vetëm të një pjese të tij ose të një mjeti tjetër memorizimi të dhënash;
b) për të nxjerrë dhe marrë kopje të të dhënave kompjuterike;
c) për të penguar hyrjen në të dhënat kompjuterike, ose për t'i hequr këto të dhëna nga sistemet kompjuterike me të drejtë hyrjeje;
ç) për të siguruar paprekshmërinë e të dhënave përkatëse, të memorizuara.
4. Për zbatimin e këtyre veprimeve, prokurori mund të urdhërojë thirrjen e një eksperti, i cili ka njohuri rreth funksionimit të sistemeve kompjuterike apo të masave të zbatuara për mbrojtjen e të dhënave kompjuterike në të. Eksperti i thirrur nuk mund të refuzojë detyrën pa shkaqe të arsyeshme.

6 Neni 151 Marrja e provave
1. *Gjatë hetimeve paraprake provat merren nga organi që procedon, sipas rregullave të caktuara në këtë Kod.2. Në gjykim provat merren me kërkesën e palëve. Gjykata vendos menjëherë, dukepërjashtuar provat e ndaluara nga ligji dhe ato që janë haptazi të panevojshme.*

sistemet komjuterike. Por moment procedurial kur mund të merren provat me kërkese të viktimës akuzuesevjen pas disa seancash gjyqësore, sic është seanca e pajtimit[7], seanca e thirrjes së prokurorit[8]dhe pastaj vazhdon me seancën e marrjes së provës, çka do të thotë që marrja e këtyre të dhënave nga sistemet komjuterike mund të bëhet i pamundur për shkak të elementit kohë dhe zhdukjes së këtyre të dhënave. Kjo sjell dështimin e viktimës akuzuese në procesin e të provuarit.

Marrja e evidencave n I KEDNJ, pavarësisht se në anën tjetër kërkohen normimi I ndërhyrjesnë sistuata të tilla për të krijuar një ballancim dhe evitim të abuzimeve të mundshme. Vetë GJEDNJ në juridiksionin e saj lidhur me zbatimine nenit 8 të KEDNJ shprehet mbi gaarancitë dhe respektimin që duhet ti bëhet kësaj dispozite dhe detyrimeve që rrjedhin nga kjo e fundit. Por njëkohësisht në anën tjetër shpjegon se ka raste përjashtimore kur mund të devijohet nga garancitë e këtij neni, raste të justikfikueshme që legjitimojnë ndërhyrjet. Raste të tilla nuk mund të konsiderohet cënim I të drejtave dhe garancive që rrjedhin nga neni 8 në momentin që plotësojnë 3 kushte kumulative:

- *Ndërhyrja të justifikohet nga një qëllim legjitim*
- *Të realizodhet ndërhyrja në përputhje me parashikimet ligjore*. Në një praktikë të GJEDNJ ku një i mitur kishte rënë pre e një pedofili nëpërmjet një publikimi nëëeb, viktima nuk arrinte të nisej një procedim ndaj askujt pasi legjislacioni i shtetit nuk e parashikonte mundësië që gjykata tu kërkonte shërbimeve të internetit të mund të identifikonin subjektin që kishte bërë një postim të tillë.[9]GJEDNJ në këtë vendim u shpreh mbi detyrimin pozitiv që kanë shtetet ne garantimin dhe mbrojtjen e kategorive vulnerable kundrejt krimit që zhvillohet nëpërmjet teknologjise. Zhvillimii teknologjisë sjell dhe efektet e saja negative në shoqëri e cila gjen terren dhe zhvillohet duke gjetur dhe prekur sipas rastit viktimat e saja. Dhe ndaj krimve që kryennëpërmjet

7 Neni 338 Përpjekja për pajtim*1. Në rastin e veprave që ndiqen me kërkesën e viktimës akuzuese, gjykata thërret viktimën dhe atë kundër të cilit është bërë kërkesa për gjykim dhe u propozon zgjidhjen e çështjes me pajtim. Në qoftë se viktima e tërheq kërkesën dhe ai që akuzohet e pranon tërheqjen, gjykata vendos pushimin e çështjes. Në të kundërtën ajo cakton datën e seancës dhe u bën të njohur atyre se mund të ndihmohen nga mbrojtës.*

8 Neni 59 Viktima akuzuese 1. *Ai që është dëmtuar nga veprat penale të parashikuara nga nenet 90, 91, 92, 112 paragrafi i parë, 119,119/b, 120, 121, 122, 125, 127, dhe 254 të Kodit Penal ka të drejtë të paraqesë kërkesë në gjykatë dhe të marrë pjesë në gjykim si palë për të vërtetuar akuzën dhe për të kërkuar shpërblimin e dëmit.*
2. Prokurori merr pjesë në gjykimin e këtyre çështjeve dhe, sipas rastiët, kërkon dënimin e të pandehurit ose pafajësinë e tij

9 ECHR K.U. v. Finland

teknologjisë si në cdo veprimtari tjetër kriminale konstatojmë viktima të cilat mund të konsiderohen më vulnerable kundrejt të tjerëëve sic janë fëmijët kryesisht.

- *Të jetë e domosdoshme për interesin që mbron***.**

Juridikksioni i GJEDNJ ka ecur në linjën e balancimit të të drejtave si ato që rrjedhin nga neni 8 I KEDNJ, por dhe duke përcaktuar qartë që veprimtari të paligjshme nga autorët të kryhen dhe të shmangen përgjegjësistë duke u justifikuar nga neni 8 i KEDNJ-së.

Në rastin Delfi AS vs Estonia, gjykata u shpreh lidhur me një nga të drejtat që vjen si rrjedhoje e nenit10 të KEDNJ, e drejta e lirisë së fjalës dhe shprehjes,[10] u shpreh se fjalime raciste dhe gjuha e urretjes dhe dhunës që cënon integritetin dhe personalitetin e individit duhet të ndalohen dhe se në asnjë mënyrë nuk bien nën objektin e nënit 10 dhe 8 të KEDNJ-së.

KONLUZIONE DHE REKOMANDIME

Kodi i Proçedurës Penale solli më shumëgaranci për viktimën e veprës penale.

Nga sa më sipër konludojmë se Kodi i Pr.Penale, nuk ka garantuar një mbrotje unifirome për viktimën e veprës penale nga vepra penale të kryera nga teknologjia dhe interneti.

Pasi për kundravajtjen penale të fyerjes npm teknologjisë dhe ato të ndërhyrjes së padrejtë në jetën private, viktima gjendet e vetme për të bërë të mundur marrjen e këtyre të dhenave.

Tek veprat penale që ndiqen me ankim nuk kemi asnjë vepër penale që

10 "*The Court notes at the outset that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognised by the Court on previous occasions (see Ahmet Yıldırım v. Turkey, no. 3111/10, § 48, ECHR 2012, and Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom, nos. 3002/03 and 23676/03, § 27, ECHR 2009). However, alongside these benefits, certain dangers may also arise. Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available on line. These two conflicting realities lie at the heart of this case. Bearing in mind the need to protect the values underlying the Convention, and considering that the rights under Article 10 and 8 of the Convention deserve equal respect, a balance must be struck that retains the essence of both rights. Thus, while the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights."*

kryhet nga teknologjia dhe informacioni, për të cilat prokurori heton pas ushtrimit të ndjkejes penale nga viktima.

Për sa më sipër, mendojmë që K.Pr. Penale, viktimës akuzuese nuk i ka dhënë shumë mjete efikase për të provuar veprën penale, duke e lënë atë të vetëm për të mbledhur provat.

Viktima akuzuese si pjesë e viktimës në tërësi ka barrën e provës për të provuar para gjykatës, kryerjen e veprës penale dhe të autorit, edhe për kundravajtje penale që kryhen nga teknologjia dhe informacioni sic janë ato tëfyerjes 119/b, Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik dhe 121 të Kodit Penal dhe ndërhyrje të padrejta në jetën private, të kryera këto nëpërmejt teknologjisë së informacionit dhe internetit. Rregullimet aktuale të nenit 208/a të KPr.Penale, nuk i japin mundësi viktimës akuzuese të ketë mundësi të marrë të dhënat komjuterike nëpërmjet këtij mjeti të kërkimit të provës. Pasi ky rregullim specific parashikon vetëm gjykatën e cila me vendim mund të urdhërojë marrjen e të dhënave komjuterike dhe ekzekutimi bëhet nga prokurori dhe opgj i deleguar nga ky i fundit. Pritja deri në momentin e marrjes së një autorizzimi të tillë mund të riskojë marrjen e provave të cilat në botën virtuale mund të ndryshohen apo fshihen shumë lehtë, duke humbur në këtë mënyrë gjurmën e hetimit dhe identifikimit të autorëve

Pra K.Pr.Penale nuk i jep mundësi viktimës pasi nuk e njef si subjekt që mund të marrë prova edhe pse ajo ka barrën e provës për të marrë prova dhe për të provuar akuzën.

Në këtë këndvështrim përfshirja e kundravajtjeve penale tëfyerjes 119/b, Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik dhe 121 të Kodit Penal, ndërhyrje të padrejta në jetën private në nenin 59 të K.Pr. Penale, nuk i jep shumë mbrotje viktimës së veprës penale për këto vepra penale. Një zgjidhje do të ishte përfshirja e këtyre kundravajtjeve penale tek nenin 284 i K.Pr.Penale. Pasi ushtrimi i ndjekjes penale për këto kundravajtje bëhet vetëm me vullnetin e vikimës së veprës penale dhe është kjo e fundit që e fillon dhe e vazhdon. Më tej veprimet hetimore kryhen nga prokurori, i cili sipas nenit 208/a të K.Pr.Penale, mund ti bëj kërkesë gjykatës për të marrë të dhëna nga sistemet kompjuterike. Prandaj në këtë këndvështrim ky rregullim ligjor do të ishte me garanci për viktimën e veprës penale, pasi ai vetëm do të bënte ankim për fillimin e ushtrimit të ndjekjes penale dhe më tej mbledhja e provave do të bëhej nga prokurori si subjekt që mbledh prova.

REFERENCAT:

- Kushtetuta e Republikës së Shqipërisë;
- Konventa Europiane e të Drejtave të Njeriut.
- Deklarata e Kombeve të Bashkuara mbi të Drejtat Themelore të Viktimave të Krimit dhe Keqpërdorimit të Pushtetit, e vitit 1985
- Direktiva e BE mbi viktimën
- Kodi i Procedurës Penale të Republikës së Shqipërisë;
- Udhëzimin e Përgjithshmë nr. 5, datë 26.10.2018 të Prokurorit të Përgjithshëm "Për garantimin e asistencës ndaj viktimave dhe dëshmitarëve të veprave penale" ka bërë një analizim të detajuar të viktimes së veprës penale
- https://www.echr.coe.int

K.U. v. Finland

Delfi AS vs Estonia

LEGAL PROTECTION FOR INTELLECTUAL PROPERTY RIGHTS IN THE DIGITAL MARKETS: AN OVERVIEW OF THE AVAILABLE LEGAL REMEDIES AGAINST ONLINE RADEMARK INFRINGEMENT

PH.D. ETLON PEPPO
Faculty of Law, University of Tirana
etlon.peppo@fdut.edu.al

PROF. ASOC. JOLA BODE
Faculty of Law, University of Tirana
jola.xhafo@fdut.edu.al

Abstract

Intellectual property rights, which include the rights deriving from the registration of trademarks, patents, utility models, industrial designs, geographical indications, denominations of origin, copyright, plant varieties, integrated circuits and trade secrets in some jurisdictions, are considered as capital assets representing the creations of the human mind. Such rights enable the owners to have exclusivity over their creations and prohibit third parties from using the said rights without the consent of the right-holder. For that reason, a specific national and international legal framework has been adopted to ensure and guarantee the protection of these important rights. Intellectual property plays an important role for the economic life and our society in general, but the huge development of the technology and the new digitalization process have been broadly exploited to infringe the IP rights. In particular, this paper is more focused on the trademark rights that have been subjected to the online infringement and other types of illegal activities using technology or internet as a tool for reaching their goals.

In this context, the global situation caused by COVID-19 has increased even more the interconnectedness of people through technology and even the number of trademark infringement cases across the globe. But, certain types of trademark infringements could also amount to a criminal offence and are often closely linked to organized crime, smuggling of goods and money laundering. Digital economy and the internet of things represent the perfect tool for the infringers to benefit from exploiting the trademark rights and engage in criminal activity. In the first place, this paper describes the legal concept of IP rights and analyses the elements of the IP crime under the criminal law. Within the digital economy environment, the paper outlines the applicable legal remedies for prosecuting and combatting online trademark infringement and all the other related economic crimes. In order to identify the main finding and conclusions on this topic, we used the most practical methods in our field research study: the doctrinal legal research methodology, the interdisciplinary research method and the analytical legal research method.

Key words: Intellectual property rights, intellectual property crime, digital economy, online trademark infringement, criminal law

I. Introduction

Intellectual property rights (hereinafter also referred as “IP rights” or “IPR”) are the rights given to persons over the intellectual creations of their minds. They give authors certain exclusive rights over the use of their creations and enable them to prohibit third parties from using their creations without authorization. The recent case-law of the European Court of Human Rights has addressed the concept of IP rights as property rights, which should be protected in the same manner as the property in possession of an individual or a legal person. IP rights constitutes an important asset for their creators and the entire society in itself. In this aspect, such rights contribute to the social and economic development of the society and the infringement of IP rights may cause a serious risk to the public interest as well.

Thus, legal protection of the intellectual property has significant importance for modern states and it has both global and national components. Global economic aspects of the IPR protection includes fulfillment of all basic principles of the multilateral conventions and adoption in the national legislation. Due to the changes in modern economy and business strategy,

new legal tools of protections are introduced.[1]

In view of the above, states have cooperated with each-other and have adopted several international agreements aiming to protect and safeguard the intellectual property rights. Some of the most important international legal agreements in the field of IP rights are the Paris Convention for the Protection of Industrial Property, 1883 (as amended) (hereinafter also referred as "Paris Convention"), the Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994 (hereinafter also referred as "TRIPS Agreement") and the Berne Convention for the Protection of Literary and Artistic Works, 1886 (as amended) (hereinafter also referred as "Berne Convention"), which have been ratified by most of the states in the World.

Such legal instruments set the minimum standards to ensure the protection of IP rights and requires the state parties to adopt effective and adequate legal remedies against infringements and unfair competition in their internal legislations. For that reason, states have adopted various administrative, civil and criminal legal remedies to safeguard the interests of IP right-holders and general public in an appropriate manner. Of course, each of these legal remedies has its own particularities and may be available for use under certain conditions provided by law.

But nowadays, the huge developments of technology and digital economy, the digital marketing and online social media have cast doubt about the efficacy of certain legal remedies against online infringements. In particular, the global situation caused by COVID-19 has increased even more the interconnectedness of people through technology and the use of digital marketing by raising the number of trademark infringement cases in a significant manner.

This paper is so more focused on the legal protection and the available remedies against online trademark infringement, which could constitute a criminal offence under certain circumstances. IP crime does not simply constitute an economic crime in terms of criminal law, but some types of trademark infringements are often linked to organized crime, smuggling of goods, money laundering and other criminal offences in the field of customs and taxes.

In the light of the above, this paper does initially give the concept

1 "Different legal aspects of the intellectual property rights"- EU and Comparative Law Issues and Challenges Series (ECLIC), Dijana Janković, University Josip Juraj Strossmayer of Osijek & Faculty of Law Osijek, 2017, Osijek, page 144, doi.org/10.25234/eclic/6526 (dated 15.06.2022).

definition of IP rights in order to understand the nature and particularities of these rights when analyzing the elements of IP crime under the criminal law. The analysis of the elements constituting an IP crime provides then a better understanding of the legal remedies available for combatting infringement, and in particular, the online trademark infringement.

Legislators are currently emphasizing the necessity of enhancing enforcement, and are looking for ways to introduce new, or increase existing, sanctions for IP infringements. Most frequently, introduction of additional criminal penalties is one of their options and is considered as one of the most effective means of enforcing intellectual property rights.[2]

Thus, this paper emphasizes the importance of criminal law in prosecuting and combatting the illegal activities amounting to a criminal IP infringement and its link to other serious economic crimes. In the final part of this paper, it is addressed the issue of the legal protection against online trademark infringement as one the most common type of IPR infringement.

Regarding this aspect, the paper outlines the best effective legal remedies available for online trademark infringement by reaching a conclusion that criminal law plays an important role in case the administrative and/or civil remedies are not sufficient to deter the illegal activity.

II. What are intellectual property rights?

Intellectual property rights are the rights given to persons and/or inventors over the intellectual ceations of their minds, including literary and artistic works, inventions, designs, names, distinctive signs and symbols used in commerce. The importance of IP rights is essential for their creators and the entire society due to the contribution that such rights bring to the social and economic development, as well as to the stimulation of the innovation and creativity.

The legal protection of IP rights encourages inventors and/or creators to develop their intellectual creations and ensures them that their new creations will be protected. For instance, the invention of the COVID-19 vaccine has been successfully protected through the worldwide patent registration, and the inventors and/or the applicants were thereby able to keep their invention safe.

2 Criminal Enforcement of Intellectual Property – A handbook of Contemporary Research, Christophe Geiger, Edward Elgar Publishing Limited, 2012, Cheltenham (UK), page 2.

In fact, intellectual property rights are divided into two main categories:

(i) Industrial Property Rights, which generally includes rights derived from the registration of trademarks, industrial designs, patents of invention, utility models, geographical indications, denominations of origins and other similar rights (plant varieties, integrated circuits or even trade secrets in some particular jurisdictions); and

(ii) Copyrights and rights related to copyright, which generally includes literary and artistic works, such as: books, music, paintings, sculpture, films, writings, computer programs and databases.

With respect to the nature of these rights, IP rights are private rights and their protection is mainly ensured through the intellectual property law. Since 1990, the case-law of the European Court of Human Rights has accepted that certain intellectual property rights are qualified "as possession" in the terms of the European Convention on Human Rights ("ECHR") and its Protocol no. 1.

Namely, article 1 of Protocol no. 1 of the European Convention on Human Rights provides that every natural or legal person is entitled to the peaceful enjoyment of his possessions[3]. In view of this provision, the right to property has been now considered to include even the creations of human mind such as: copyright, patents, trademark, etc. Therefore, the competent authorities have the positive obligation to take all the necessary measures to ensure the right to property.

On the international level, many authors have affirmed that IP rights enjoy a specific protection by the Universal Declaration of Human Rights (UDHR). Likewise, the World Intellectual Property Organization ("WIPO") has underlined in its manuals that intellectual property rights are safeguarded by Article 27 of the Universal Declaration of Human Rights[4]: Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.[5]

In order to ensure the protection of the intellectual property rights, states have also cooperated with each-other and have adopted several international

3 Article 1 of Protocol no. 1 of the ECHR: *Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.*

4 What is intellectual property?, World Intellectual Property Organization, WIPO Publication, 2020, Geneva, page: 2.

5 Article 27 of the Universal Declaration of Human Rights, 1948.

agreements in this respect. Some of the most prominent international legal agreements are the Paris Convention, TRIPS Agreement and the Berne Convention. All these important instruments set out the minimum standards, while the contracting state parties are required to adopt effective and adequate legal remedies against infringements and unfair competition at national level.

The said agreements provide the necessary measures to enforce the trade-related intellectual property rights and set forth various civil, administrative and criminal legal remedies against the infringement of IP rights from third parties. Administrative and civil remedies are generally used by the trademark owners to demand compensation for an infringement, injunctions halting further infringements and other similar measures (including the imposition of administrative fines).

As regards for the criminal legal remedies, which constitute an essential part of this paper, the TRIPS Agreement has the added significance of being the first international legal instrument that determine that states have the obligation to criminalize the infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

Namely, article 61 of TRIPS Agreements requires member states to provide and apply for criminal procedures and penalties at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale.[6] According to the same article, criminal legal remedies shall necessarily provide the imprisonment and/or monetary fines. Other available and possible criminal remedies include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence.

While it should be underlined the fact that the TRIPS Agreement allows the member states to provide and apply for criminal procedures and penalties in case of infringement of other types of intellectual property rights, this paper will focus on the online trademark infringement and will provide an overview of the legal protection available against this common type of infringement in the digital marketplace.

III. Intellectual property crime and its link to other economic crimes: The importance of criminal law

IP crime is not just an economic crime, and the infringement of intellectual

6 Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994.

property rights does often link in a close manner to other serious crimes such as: the organized crime, corruption, money laundering, smuggling of goods or other criminal offences in the field of taxes and customs. In view of this matter, this paper aims to point out the relevance of criminal law in prosecuting and combatting the criminal activity in this area.

While it is true that not any IP infringement is subject to criminal law, it should be taken into account that such rights represent a public interest for the society and it might be necessary to prosecute this illegal conduct when certain conditions are fulfilled. As previously mentioned above, there are different types of legal proceedings that might be initiated against an infringer of IP rights: administrative, civil and criminal proceedings. The form of the liability depends by the infringement type and the nature of the unlawful conduct of the infringer.

As a general practice, the civil and administrative remedies are mainly used by the IP riht-holders to demand compensation for an infringement or seek injunctions halting further infringements. On the other hand, we may also conclude that criminal legal remedies are found to be more effective in cases when the administrative and civil legal remedies could not be sufficient to deter and prohibit the illegal IP activity.

Harmonization of criminal law at international and European level has been very controversial, since criminal law is closely linked to moral and cultural conceptions within a society. Criminal law has always been a tool to protect the public interest, the harm to society being the justification for the existence of a criminal penalty. Of course, these conceptions diverge severely in different parts of the worlds.[7]

Owing to the impact of IP rights in the social and economic development of a country and its close link to the other serious crimes cited above, the law enforcement agencies should be first capable to identify and analyze the essential elements constituting an IP crime. Furthermore, the investigation and the prosecution of such crimes could not be successfully conducted in case competent authorities do not have a clear overview of IP law. If this is the case, the authorities may err and wrongly assess the fact whether criminal proceedings should be initiated or if the matter of dispute belongs to the civil jurisdiction.

In the light of the above, we would like to share the experience of the US authorities in their fight against the IP crime. Namely, the FBI's Criminal

7 Criminal Enforcement of Intellectual Property – A handbook of Contemporary Research, Christophe Geiger, Edward Elgar Publishing Limited, 2012, Cheltenham (UK), page 1.

Investigative Division's Intellectual Property Rights Unit ("IPRU") oversees its national intellectual property rights program, which includes dedicated FBI Special Agents responsible for investigating (i) thefts of trade secrets, (ii) manufacturing and trafficking in counterfeit goods, and (iii) IPR infringement, which causes significant economic impact.[8] From this point of view, it is quite evident the importance given to such types of infringements in a developed economy such as US.

In some cases, the infringement of intellectual property rights may pose a very high risk to the life and health of individuals. For example, counterfeiting activity constitutes an infringement of trademark rights and it may concern different types of goods, such as: pharmaceuticals, parts for automobiles and planes, food items or alcoholic drinks. Under these circumstances, the US Department of Justice rightly asserts that the impact of today's IP crime is not limited to the economic challenges associated with piracy, counterfeiting, or trade secret theft. Inferior, unsafe counterfeits, ranging from electrical equipment to auto parts to pharmaceuticals, not only defraud ordinary consumers, but also can pose significant risks to their health and safety.[9]

Criminal law not only plays an important role when the IP infringement invokes public interests, but also when the commitment of such infringement is linked to other economic and financial crimes. In this context, several reports and researches have evidenced that any use of money derived from certain types of IPR violations to fund specific forms of crime is considered money laundering.[10]

To ascertain the link between the infringement of intellectual property rights and other economic or financial crimes, we should take into account that IPR infringements facilitate the commitment of other crimes such as: tax evasion, smuggling, organized crime, cybernetic crime, fraud, etc. The profits from the products infringing intellectual property have begun to exceed the profits from drugs and weapons on the profit/weight basis

8 Reporting intellectual property crime - A guide for victims of copyright infringement, trademark counterfeiting, and trade secret theft (third edition), US Department of Justice, Computer Crime and Intellectual Property Section, 2018, page: 10, www.justice.gov/criminalccips/.ccips-documents-and-reports (dated on 16.06.2022).

9 Prosecuting intellectual property crimes (fourth edition), US Department of Justice, Office of Legal Education Executive Office for United States Attorneys, 2017, page: 2.

10 Intellectual Property and White-collar Crime: Report of Issues, Trends, and Problems for Future Research, National White Collar Crime Center, 2004, https://www.ncjrs.gov/pdffiles1/nij (dated on 16.06.2022).

and always due to lower penalties.[11] This is probably the reason that such crimes have become so attractive for the organized crime groups, which have increased their profits due to the trade of products infringing the intellectual property rights.

Also, it should be noted that the infringement of IP rights is very often linked with smuggling of goods and the circulation of counterfeit or copyright piracy goods at the customs borders. With respect to this matter, customs authorities are inclined to refer the illegal activity concerning the smuggling of goods to the Prosecution Office and no reference is made to the infringement of IP rights. In such a case, the infringement of IP rights constitutes a criminal offence and it should be referred to the Prosecutor Office as well.

Another criminal offence linked to the IP crime is the cybercrime. Organized crime groups or even individuals exploit the facilities provided by the internet and social media platforms to infringe intellectual property rights and gain financial profit to the detriment of IP authors and owners/ licensees.

An example from the recent judicial practice to show how IP crime is linked to the economic crimes defined above is the recent police operation named "Online websites" taken by the Economic Crime Division within the Tirana Police Office under the direction of the Tirana Prosecution Office. The criminal investigation of the case revealed that 15 persons advertised and traded different goods through their online pages on the social media, goods which were suspected to have entered into Albania as smuggle goods. As regards their sale, no tax invoice was provided by the sellers to the buyers.

In view of the above, all the arrested persons were charged with the criminal offences of "Infringement of industrial property rights", "Smuggling of other goods", "Tax evasion" and "Failure to pay taxes". As material evidence, the Prosecution Office in charge has seized all the goods intended to be traded and distributed by mail.

As a matter of procedural law, IP crimes are generally prosecuted when a private party lodges a complaint for infringement of IP rights before the Prosecution Office or the Economic Crime Division at the Police Office.

11 Hetimi dhe ndjekja e veprave penale që lidhen me pronësinë intelektuale në Shqipëri: Manual për trajnimin e prokurorëve, gjyqtarëve dhe autoriteteve të tjera ligjzbatuese [*Criminal investigation and prosecution of the criminal offenses related to intellectual property in Albania: Handbook for training of the prosecutors, judges and other law enforcement agencies*], Mariana Semini-Tutulani, WIPO, 2020, Geneva, page: 14.

Aside from the standard concerns about overcriminalization and the more specific concern about over-deterring potentially beneficial uses, in the IP context one important consequence of the expansion of criminal liability is that it shifts the burden of enforcement from private parties to the public.[12]

As a conclusion, we may say that criminal law plays an important retributive, preventive and educational role through the provision of the criminal offence for the infringement of IP rights and the relevant sanctions against the perpetrators.

The criminal sanctions for committing IP crimes consist of imprisonment and/or fine. In the majority of cases, the competent judicial authorities may also impose the seizure, forfeiture and destruction of the infringing goods and of any materials or instruments related to the commission of the offence.

IV. Legal protection against online trademark infringement: which are the best effective legal remedies?

International property crime is committed when someone manufactures, sell or distributes counterfeit or pirated goods, such as trademarks, patents, industrial designs or copyright, for commercial gain. If the commercial purpose is missing, as for example in the case when the manufacture or sale of these goods is committed for personal use and not for commercial purposes, the author should not be held criminally liable.

Digital economy and the internet have become an important factor for economic growth, but they have also facilitated illegitimate commerce and the sale of counterfeit goods to the detriment of consumers and IP rights owners. In particular, internet and digital markets serve as the perfect tool for the infringers to benefit from illegally exploiting the trademark rights and engage in criminal activity.

The owner of a registered trademark has an exclusive right in respect of the mark: the right to use the mark and to prevent unauthorized third parties from using it, or a confusingly similar mark, so as to prevent consumers and the public in general from being misled. The period of protection varies, but a trademark can be renewed indefinitely on payment of the necessary fees and on condition that the mark is used.[13]

12 Criminal Trademark Enforcement and the Problem of Inevitable Creep, Mark McKenna, 51 Akron L. Rev. 989, 2017, page 1023. https://scholarship.law.nd.edu/law_faculty_scholarship/1360 (dated 18.06.2022).

13 Understanding Intellectual Property (second edition). World Intellectual Property Organization,

In fact, trademarks are found everywhere: on the Internet, supermarkets, shops, boutiques, radio, TV, Facebook, Instagram, newspaper, etc. But, what is trademark in intellectual property law? A trademark is a sign capable of distinguishing the goods and/or services of one enterprise from those of other enterprises.

The above legal definition for trademarks, which is essential to be understood correctly by the law professionals, sets out the importance of protecting such rights:

Trademarks identify the source of origin of goods and/or services of a particular undertaking: This function enables the consumers to choose their preferred products when buying certain goods or services, as well as the distinctive character of the company is evidenced.

Trademarks serve as a guarantee of quality for the concerned goods or services: Consumers can rely on the quality of the goods or services based on their trademark. Moreover, the owner of a registered trademark may grant a license to the licensee by requiring the latter to respect and maintain the same quality standards.

Trademarks promote the sale of goods and the provision of services:

This function, also known as the communication function, enables the owners of trademarks to stimulate sales in the market through the associated trademark. Trademarks create interests and bring appeal to the consumers.

Any form of unauthorized use of the trademark, including the online trademark use, may potentially constitute a trademark infringement. In particular, online infringement may take many different forms. Examples include:

Sales of counterfeit or infringing products through direct sites or counterfeit sites;

Use of the same or similar marks in advertisements or promotions;

Integration of trademarks in domain names or social media handles;

Impersonation of a brand owner's website or social media pages;

Impersonation of a company's personnel; and

Use of proprietary images or content.[14]

WIPO Publication, 2016, Geneva, page: 10.

14 Combatting online Infringement: Real-world solutions for an evolving digital world. Erica

Moreover, trademarks are of essential importance in e-commerce. It is clear that trademark carry at least as much significance on the Internet as in the off-line world. Consumers, operating in virtual markets where face-to-face interactions are infrequent and there is little or no opportunity to inspect goods or services before purchase, are willing to reward trusted sources offering competitive products.[15]

Today, online counterfeiting is one of the most significant issues that trademark owners and law enforcement agencies are dealing with everywhere in the world. The huge impact of technological developments and the new digital transformation have been broadly exploited to infringe the rights of trademark owners with the aim of making illegal profits. In addition, the pandemic situation caused by COVID-19 increased the risk of IP infringing activity and determined a new trend of the criminality in this field.

International trade in counterfeit products has been estimated in the value of EUR 338 billion and has an impact on the revenues of the affected businesses, loss of jobs and health or safety standards for consumers. Infringers exploit the Internet, social media platforms and e-commerce websites to sell and trade counterfeit goods to a very large scale of audience.

Owing to the special nature of this type of infringement, this paper is especially focused on the legal remedies available for protecting trademark rights and their effectiveness to reach a satisfactory resolution. Specifically, a special attention has been paid to the criminal law as a tool for combatting the IP crime, cybercrime and other related criminal offences linked with the infringement of trademark rights.

While there are many similarities how the legal protection of trademark rights should be addressed when the infringement is committed online and offline, it should be also noted that the effectiveness of the legal remedies available for the IP rights owners is not the same. However, there is a general international consensus that trademark protection under law should extend to the Internet, and that its scope should be neither less nor more extensive than the protection granted in the physical world.[16]

Notice and takedown mechanisms may be a very effective measure if

D. Klein and Anna K. Robinson. Landslide, Vol.12, No.4, March/April 2020, https: www.americanbar.org (dated on 20.06.2022).

15 Intellectual Property on the internet: A survey of issues, World Intellectual Property Organization, WIPO Publication, 2002, Geneva, page 42.

16 Intellectual Property on the internet: A survey of issues, World Intellectual Property Organization, WIPO Publication, 2002, Geneva, page 42.

the infringement is minor. In this respect, all the online platforms and social media pages have introduced this possibility for business and consumers in order to regulate the online activity and obtain a prompt solution against the online infringement of IP rights. These mechanisms are now easily accessible and offer the opportunity to gain remedy without incurring to litigation costs.

Administrative fines seem to be not so effective against trademark online infringement, while there are enormous difficulties to identify the infringer behind a social media page or a website. Since the counterfeit or pirated goods are delivered by mail, the customs measures might represent an effective legal remedy. Customs law allows the IP right-holders to file a customs application with the customs authorities by submitting all the necessary information to enable the letter to distinguish the genuine goods and seize the counterfeit ones infringing their IP rights.

As regards for other administrative legal remedies, the role of the State Inspectorate of Market Surveillance is quite limited due to the online type of infringement. On the other hand, the Domains Authority bears an important responsibility in the fight against online trademark infringement by preventing registered trademarks from being illegally used as domain names.

But, as a matter of fact, trademark owners prefer to file civil actions against the infringers in order to cease the infringement and seek compensation for the damages. These civil remedies may include the possibility to file lawsuits, injunction requests or create deterrence. The civil legal framework enables the IP right-holders to obtain a court decision and remove all the materials, instruments, devices and other means that are used to manufacture the infringing goods from the civil circulation.

To make possible an immediate response against an online infringement, IP owners may request and obtain a court injunction ordering the Internet Service Providers (ISP) to take measures to remove, block or disconnect the infringing links. In this context, website blocking injunctions represent a new effective and useful legal remedy against online infringers where the issue of a "take-down notice" has not been effective in deterring further infringement. ISP may be so requested to block content when they are aware about the infringing content.

With respect to the counterfeit goods traded online, it is not sufficient to simply remove or detach the trademark/sign that is attached to these goods. Additionally, IP right-holder may also ask for indemnification and request

to have the court decision published in the public media at the expenses of the infringer.

In many cases, both the administrative and civil legal remedies are not sufficient to create deterrence. Infringers are inclined to not stop their infringement activity by benefiting from the development of the technology and use other means to infringe trademark rights. In such cases, trademark owners agree that the deterrence to trademark infringement may be effectively ensured by means of criminal legal remedies.

The biggest problem that blocks criminal investigations against online sellers is the anonymity of the online marketplaces that they hide behind. Anonymity is an obvious advantage for an offender, and digital technology facilitates this in a number of ways. Offenders may deliberately conceal their identity online by the use of proxy servers, spoofed email or internet protocol (IP) address or anonymous emailers. Simply opening an email account which does not require identity verification provides a false identity.[17] Therefore, it is essential to first identify the person standing behind the online marketplace selling infringing goods and the help of the Internet Service Provider is needed for this important step of enforcement.

A person may be found liable for an IP crime if the prosecution proves that both the physical element (actus reus) and the mental element (mens rea) are satisfied. In view of this analysis, the online trademark infringement as a criminal offence may be committed through various forms and methods related to the unauthorized online distribution, sale, offer for sale, supply, export or import for commercial purposes of the goods protected by a trademark.

Also, the mental element is considered as satisfied when the IP crime is committed willfully and for commercial purposes. As a conclusion, it is important to emphasize that it might happen that a person is not held criminally liable for an IP crime due to the lack of guilt, but he/she might be still found responsible for the infringement of IP rights by a civil court.

Since IP crimes are generally prosecuted when a private party lodges a complaint for infringement of IP rights before the Prosecution Office or the Economic Crime Division at the Police Office, the latter shall investigate and initiate the criminal proceedings against the infringer of trademark rights in case the legal requisitions for criminal prosecution are met.

17 Principles of cybercrime - Second edition, Jonathan Clough, Cambridge University Press, 2015, Cambridge, page 7.

As mentioned above, the identification of the infringer is absolutely not a simple task. For that reason, a qualified technical training and expertise should be provided to law enforcement agencies. On the other hand, the preservation of evidence during the prosecution of these criminal cases is also of a huge importance.

Above all, the trademark owners should fully and closely cooperate with the police officers/prosecutor. All the information and documents in their possession should be made available to the authorities in charge of the criminal prosecution. If we are in front of a persistent and severe infringing activity, criminal actions and its related legal remedies might be the best effective way to prohibit and deter the infringement of trademark rights.

Generally, it exists a distinct line between the administrative, civil and criminal sanctions that are applied against the infringers of trademark rights. For instance, in China, Administrative punishments may be imposed according to relevant laws and regulations on common IPR violations that are inadequate to be deemed crime, and criminal punishments are imposed in the cases where serious harm has been done to the society and the amount involved in the violation or the loss caused to the victim reaches the threshold for prosecution.[18]

V. Conclusions

Intellectual property rights, which include the rights deriving from the registration of trademarks, patents, utility models, industrial designs, geographical indications, denominations of origin, copyright, plant varieties, integrated circuits and trade secrets in some jurisdictions, are exclusive rights given to persons over the intellectual creations of their mind. Such rights contribute to the economic and social development of the society, as well as encourages innovation and technology development. In this context, IP rights have a great importance for both their owners and the public interest.

For that reason, states have adopted a special legal protection in an international and national level with the aim to guarantee these rights from third party infringements. As result, various administrative, civil and criminal legal remedies have been adopted into their domestic law by states. In the recent years, the risk for infringement of IP rights has increased

18 "Intellectual Property Rights Protection through Criminal Justice in China, Current Situation and Prospects" Speech at the Third Global Congress on Combating Counterfeiting and Piracy, Xiong Xuanguo, 2007, Geneva, page:2,https://www.wipo.int/edocs/mdocs/enforcement/en/third_global_congress/third_global_congress_ref_f.pdf. (dated 20.06.2022).

significantly due to the huge development of the technology, social media pages and Internet in general. Particularly, the pandemic situation caused by COVID-19 disease has contributed even more to increase the number of online trademark infringement cases.

Under certain circumstances, some types of trademark infringements could also amount to a criminal offence. In many cases, IP crime is often linked to the organized crime, smuggling of goods, money laundering, evasion of taxes and cybercrime. Therefore, criminal law may so play an important retributive, preventive and educational role in the fight against trademark infringement.

Online trademark infringement is currently one of the most common intellectual property rights infringement, whereas the e-commerce platforms and social media pages have been particularly exploited as a perfect tool to sale counterfeit foods worldwide. While it is true that there is little or no opportunity to inspect goods or services when purchasing them online, there is also a general international consensus that trademark protection under law should extend to the Internet, and that its scope should be neither less nor more extensive than the protection granted in the physical world.

But, which are the legal available remedies against online trademark infringement? A trademark is a sign capable of distinguishing the goods and/or services of an undertaking from those belonging to another undertaking, and the legislator should adopt adequate and effective legal remedies to ensure the protection of trademark rights online and in the physical world.

Notice and shutdown mechanisms may be a quick and effective solution when the infringement is minor. For that reason, all the e-commerce platforms and social media pages have introduced this mechanism in their policies and enable IP owners to obtain a prompt solution without incurring to litigation costs.

Administrative fines are generally not so effective, while the infringers are keen to avoid the payment of fines due to their operation on the online network. The involvement of the State Inspectorate of Market Surveillance might not produce results based on the type of infringement, but customs measures could perfectly serve as an effective tool to combat the illicit counterfeiting activity of goods that are sold online. Also, the Domains Authority may be helpful in the fight against online trademark infringement by preventing registered trademarks from being illegally used as domain names.

Actually, IP owners prefer to file civil actions against infringers to cease the infringement and seek compensation for the damages. Apart from filing a lawsuit for trademark infringement and seeking compensation for the damages, civil legal remedies include the possibility to have the final court decision published at the expenses of the infringer and obtain injunctions. In particular, the website blocking injunctions are found a very effective remedy to order Internet Service Providers for taking measures to remove, block or disconnect the infringing links.

Notwithstanding from the above, administrative and civil legal remedies could not create deterrence to trademark infringement. In such cases, the aid of criminal law and the application of the criminal sanctions are the most effective enforcement measure of trademark rights.

Article 61 of the TRIPS agreement requires member states to provide and apply for criminal procedures and penalties at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Thus, criminal legal remedies provide the imprisonment and/or monetary fines, as well as the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence.

While IP crimes are generally prosecuted when a private complaint is lodged with the Police or the Prosecution Office, it should be noted that a person may be found criminally liable in case both the physical element (actus reus) and the mental element (mens rea) are satisfied. The biggest problem in the investigation of IP crime is represented by the anonymity of the infringer that stands behind the online network, the identity of which might be obtained only in case the respective Internet Service Provider manages to match the relevant Internet Protocol address of a computer used on a network with the individual subscriber and the national law allows to disclose this information.

In view of the above, we would strongly recommend that a qualified technical training and expertise should be necessarily provided to law enforcement agencies. Also, the preservation of online evidence is of a crucial importance for a successful investigation. For this purpose, enforcement officers may make undercover online purchases of goods from sellers suspected to infringe trademark rights by selling counterfeit goods.

If such goods are confirmed as counterfeit or illegal once they are delivered, a request may be field to the court in order to obtain seizure orders for the domain names of the websites selling counterfeit goods. When

possible, seizure orders may be obtained even for the PayPal accounts that are utilized by the offenders.

Some simple and common measures to be taken against the online trademark infringement include the registration of trademarks in the territories in which the business operates or intends to operate, the adoption of technological solutions such as monitoring software and the investment on watch services to be conducted by specialized trademark attorneys for IPR infringement.

Businesses should also adopt employee policies and trainings tasked with online enforcement responsibilities, which will enable their employers to handle notice and shutdown mechanisms promptly and successfully. In this aspect, it is important to underline that the recent case law of the European Court of Justice has ruled out that e-selling platforms are not liable for infringing trademark rights. In a recent case involving Amazon Europe, the ECJ concluded that Amazon merely takes care of the technical provisions and receives a compensation for those services. As far as Amazon does not market the product itself nor it intends to do so, there is no infringing use of trademarks by Amazon.

As regards for the criminal investigation of an IP crime, the identification of the offender standing behind a social media page or an online platform remains a very difficult task. But, this is not the only problem! Suing for online trademark infringement does almost always involve cross-territorial actions making it difficult to determine the applicable law, the competent jurisdiction and the enforcement of a foreign judgment in a country.

In such cases, a close cooperation between the relevant state authorities is essential for conducting the investigation and the prosecution of a criminal case. Also, such a close and a strong cooperation should be stablished even between IP owners and the enforcement officers or the Prosecutor in charge when dealing with the investigation of an IP crime. IP owners should provide all the necessary documents and information in this respect.

Owing to the close link between IP crimes and other serious criminal offences (i.e., the organized crime, smuggling of goods, money laundering or tax evasion), the police officers and the Prosecution office should be very careful to conduct a comprehensive and thorough investigation for identifying and determining the elements of all the eventual crimes that might have been committed when infringing the intellectual property rights.

In particular, customs officers should refer the case to the Prosecutor

Office properly when they detect smuggle goods at the borders. In most of the cases, offenders should be charged for both the criminal offences of "Smuggling of goods" and "Infringement of IP rights". In practice, customs officers do just refer the case to the Prosecution Office in relation to the smuggling of goods and ignore the fact that the illegal activity constitutes an IP crime as well.

Last but not least, specialized courts or specialized sections within the courts should be established to handle these matters in the most professional way possible. Meanwhile, ongoing trainings for police officers, prosecutors and judges should be more frequently organized and a specialized expertise from EU magistrates would be beneficial as well.

Bibliography

Christophe Geiger, Criminal Enforcement of Intellectual Property – A handbook of Contemporary Research, Edward Elgar Publishing Limited, 2012, Cheltenham (UK)

Dijana Janković, "Different legal aspects of the intellectual property rights"- EU and Comparative Law Issues and Challenges Series (ECLIC), University Josip Juraj Strossmayer of Osijek & Faculty of Law Osijek, 2017, Osijek.

Erica D. Klein and Anna K. Robinson. Combatting online Infringement: Real-world solutions for an evolving digital world, Landslide, Vol.12, No.4, March/April 2020.

Jonathan Clough, Principles of cyber crime - Second edition, Cambridge University Press, 2015, Cambridge.

National White Collar Crime Center, Intellectual Property and White-collar Crime: Report of Issues, Trends, and Problems for Future Research, 2004.

Mariana Semini-Tutulani, Hetimi dhe ndjekja e veprave penale që lidhen me pronësinë intelektuale në Shqipëri: Manual për trajnimin e prokurorëve, gjyqtarëve dhe autoriteteve të tjera ligjzbatuese [Criminal investigation and prosecution of the criminal offenses related to intellectual property in Albania: Handbook for training of the prosecutors, judges and other law enforcement agencies], WIPO, 2020, Geneva.

Mark McKenna, Criminal Trademark Enforcement and the Problem of Inevitable Creep, 51 Akron L. Rev. 989, 2017.

US Department of Justice, Computer Crime and Intellectual Property Section, Reporting intellectual property crime - A guide for victims of copyright infringement, trademark counterfeiting, and trade secret theft (third edition), 2018.

US Department of Justice, Prosecuting intellectual property crimes (fourth edition), Office of Legal Education Executive Office for United States Attorneys, 2017.

World Intellectual Property Organization, Intellectual Property on the internet: A survey of issues, WIPO Publication, 2002, Geneva.

World Intellectual Property Organization. Understanding Intellectual Property (second edition), WIPO Publication, 2016, Geneva.

World Intellectual Property Organization, What is intellectual property?, WIPO Publication, 2020, Geneva.

Xiong Xuanguo, "Intellectual Property Rights Protection through Criminal Justice in China, Current Situation and Prospects" at the Third Global Congress on Combating Counterfeiting and Piracy, 2007, Geneva.

Legislation

Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994.

Berne Convention for the Protection of Literary and Artistic Works, 1886 (as amended).

European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

Paris Convention for the Protection of Industrial Property, 1883 (as amended).

Protocol no. 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1952.

Universal Declaration of Human Rights, 1948.

THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN PREVENTION OF CORRUPTION IN ALBANIAN JUDICIARY SYSTEM

DR. BOJANA HAJDINI

Department of Law, Epoka University

bhajdini@epoka.edu.al

DR. GENTJAN SKARA

Department of Law, "Bedër" University College

Egskara@beder.edu.al

Abstract

Although, during these three decades, Albania has taken a number of measures to fight corruption, corruption remains a worrying phenomenon.[1] According to 2021 Corruption Perceptions Index published by Transparency International, Albania has scored 35 out of 100. In 2020, Albania was ranked in the 34th place out of 100 countries.[2] In the same vein, the 2021 Commission Progress Report noted that the impact of anti-corruption measures in particularly vulnerable areas remains limited.[3]

1 UNODC, 'Corruption in Albania: Bribery as Experienced by the Population' (2011) <http://www.instat.gov.al/media/3587/corruption_in_albania.pdf> accessed 2 June 2022, p. 7.

2 Transparency International, '2021 Corruption Perceptions Index' <https://www.transparency.org/en/cpi/2021> accessed 2 June 2022.

3 Commission, 'Albania 2021 EC Progress Report' (Communication) SWD(2021) 289 final, fq.

One of the main areas reported by Albanian citizens and international organizations as problematic is the judicial system. In the last 30 years, Albania judiciary system has undergone profound changes but has failed to gain public trust or meet international standards. While in 2016 Albanian Parliament, supported by the EU and USA, adopted a judiciary reform, still 6 years later, judiciary system is considered by citizens as corrupted. In order to increase public trust and avoid corruption, it is required to increase transparency, accountability and citizens' access to information. One way of increasing citizens' access to justice is the use of information technology.

This paper analyses the role of information and communication technology in prevention of corruption in Albanian judiciary system. The paper provides a short description of the role of information and communication technology in the area of the law, with a specific reference to judiciary system. Then the paper assesses how and to what extent information and communication technology can reduce corruption by promoting transparency, accountability, citizens' access to information.

***Key words**: Information and Communication Technology, Corruption, Albanian judiciary, prevention, transparenc*

1. Hyrje: Fenomeni i korrupsioni në Shqipëri

Korrupsioni prej vitesh listohet si një ndër problemet më shqetësuese të shoqërisë. Qytetarët besojnë se ai është një fenomen i përhapur në të gjitha sektorët, dhe së bashku me ekonominë e vendit dhe papunësinë duhet të përbëjnë një ndër prioritetet qe kërkojnë zgjidhje imediate.[4] Sipas Indeksit të Perceptimit të Korrupsionit të Transparency International për vitin 2021, Shqipëria është në listën e vendeve më të korruptuara në botë, duke u renditur e 110-ta nga 180 vende,[5] e duke shënuar një rënie prej gjashtë vendesh që prej vitit 2020. Sipas Transparency International vendi yne mori 35 pikë nga 100 të mundshme, duke u renditur në të njëjtën nivel me Bosnje dhe Hercegovinën, Malavinë, Mongolinë dhe Tajlandën, ndërkohë që lihet pas

<26file:///C:/Users/pc/Downloads/Albania-Report-2021%20(7).pdf>, accesed 2 June 2022

4 Euronews Albania, '92% e shqiptarëve mendojnë se qeverisja është e zhytur në korrupsion' <https://euronews.al/programs/shqiperi/barometri/2021/09/23/live-l-92-e-shqiptareve-mendojne-se-qeverisja-eshte-e-zhytur-ne-korrupsion/> aksesuar më 15 qershor 2022.

5 Transparency international, *Corruption Perceptions Index 2021* (Transparency International 2022) <https://images.transparencycdn.org/images/CPI2021_Report_EN-web.pdf> aksesuar më 15 qershor 2022, fq 3.

nga vende të tjera të rajonit si Kosova, Maqedonia e Veriut dhe Serbia.[6] Në një hark kohor prej 10 vitesh, Shqipëria ka pësuar rritje me vetëm dy pikë, tregues ky që masat dhe reformat e ndërmarra në vazhdimësi kundër korrupsionit, nuk kanë dhënë efektin e pritshëm.[7]

Një ndër sektorët, i cili ka një perceptim të lartë të korrupsionit është sistemi gjyqësor. Sipas anketimeve, rezulton që qytetarët, besojnë se "*proceset gjyqësore ndikohen më së shumti nga interesa monetare, lidhjet e biznesit, lidhjet personale të gjyqtarëve e prokurorëve, dhe interesat e presionet politike*".[8] Për vite me radhe gjyqësori, referuar vlerësimeve të bëra nga organizmat e huaja dhe vendase, konsiderohej si sektor me nivel të lartë korrupsioni.[9]

Edhe pse ndërkohë prej 5 vitesh është duke u aplikur Reforma në Drejtësi, ku një ndër shtyllat e saj kryesore ishte pastrimi i të korruptuarve nga rradhët e gjyqësorit, përsëri ky i fundit vijon të mos ketë besimin e qytetarëve dhe të perceptohet si ineficent dhe i korruptuar. Sipas Raportit të fundit të Departamentit Amerikan të Shtetit, korrupsioni listohet si një ndër faktorët qe penguan gjyqësorin të funksiononte, në mënyrë të pavarur dhe të efektshme.[10]

Gjithashtu, korrupsioni është një ndër pengesat kryesore për aderimin e Shqipërisë në BE. Kjo është aryeja që BE, përmes Politikës së Zgjerimit (2020), vendosi theksin në luftën kundër korrupsionit dhe krimit të organizuar, duke i konsideruar ato si kusht kryesor në forcimin e shtetit ligjor sipas Kritereve të Kopenhagës.[11] Sipas metodologjisë së fundit të

---

6 Po aty.

7 Shih për më tepër intervistën e dhënë për DW, të Lidija Prokiç, koordinatore për Evropën Lindore dhe Juglindore në Transparency International. DW, 'Lufta kundër korrupsionit është përgjegjësi e vetë qeverive të Ballkanit Perëndimor' <https://www.dw.com/sq/lufta-kundër-korrupsionit-është-përgjegjësi-e-vetë-qeverive-të-ballkanit-perëndimor/a-60553484> aksesuar më 15 qershor 2022.

8 Grupi i Ekspertëve të Nivelit të Lartë, 'Strategjia në Reformimin e Sistemit të Drejtësisë' <https://rm.coe.int/strategjia-ne-refomen-e-sistemit-te-drejtesise/16809eb53a> aksesuar më 15 qershor 2022, fq 38.

9 Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' (qershor 2015) <http://www.reformanedrejtesi.al/sites/default/files/dokumenti_shqip_0.pdf> aksesuar më 15 qershor 2022, fq 10.

10 Departamenti Amerikan i Shtetit, 'Raporti për të Drejtat e Njeriut 2021: Shqipëria' <https://al.usembassy.gov/sq/our-relationship-sq/official-reports-sq/> aksesuar më 15 qershor 2022.

11 Council of the European Union, 'Council conclusions on enlargement and stabilisation and association process - Albania and the Republic of North Macedonia' (25 mars 2020) <https://data.consilium.europa.eu/doc/document/ST-7002-2020-INIT/en/pdf> aksesuar më 15 qershor 2022, fq 5.

zgjerimit, Shqipëria deri në Konferencën e Parë të Anëtarësimit, duhet të ketë përmbushur gjashtë parakushte, dy ndër të cilat i referohen përkatësisht vijimit të zbatimit të reformës në gjyqësor, si dhe luftës ndaj korrupsionit e krimit të organizuar.[12] Në raport progresin e fundit për Shqipërinë, edhe pse pranohet që kjo e fundit ka bërë disa hapa në drejtim te luftës ndaj korrupsioni, theksohet se ai "*përsëri është i përhapur në shumë sektore të jetës publike dhe biznesit, duke mbetur një çështje shqetësuese serioze".*[13]

Në ditët e sotme, dixhitalizimi nuk është më privilegj i vendeve të industrializura. Ai po merr hov edhe në vendet në zhvillim si Shqipëria, ku teknologjia e informacionit po përdoret në të gjithë sektorët publikë, përfshi këtu edhe drejtësinë. Në këtë kontekst, është e rëndësishme që ajo të përdoret si një mjet efektiv që promovon në sistemin gjyqësor transparencën, llogaridhënien, dhe pjesëmarrjen e qytetarëve, të cilat rrisin integritetin e gjyqësorit dhe njëkohësisht parandalojnë korrupsionin në këtë sektor.

Ky punim synon pikërisht të paraqese një panoramë të mjeteve të teknologjisë së informacionit në dispozicion të gjyqësorit, të cilat ndikojnë dhe priten të sjellin impakt në parandalimin e korrupsionit në sistemin gjyqësor. Ai përbëhet nga kjo hyrje dhe 4 seksione. Seksioni i dytë trajton kuptimin e korrupsionit në sistemin gjyqësor dhe format e shfaqjes së tij. Në seksionin e tretë analizohen faktorët që kanë kontribuar në rritjen e korrupsionit në sistemin gjyqësor shqiptar. Më pas, seksioni i katërt përshkruan shkurtimisht risitë e reformës në drejtësi. Seksioni i pestë analizon mjetet e teknologjisë së informacionit në përdorim nga sistemi gjyqësor të cilat ndikojnë në rritjen e transparencës, llogaridhënies dhe përfshirjes së publikut dhe që pritet të luajë një rol të rendësishëm në parandalimin e korrupsionit në gjyqësor.

2. Kuptimi i korrupsioni në gjyqësor dhe format në të cilat shfaqet

Sipas një përkufizimi të përgjithshëm korrupsioni shihet si keqpërdorim i funksionit publik apo pushtetit të akorduar për përfitime private.[14] Korrupsioni i gjyqësorit, në këndvështrimin e qytetarit të thjeshte, asociiohet me gjyqtarin

12 Po aty.

13 Commission, 'Albania 2021 EC Progress Report' (Communication) SWD(2021) 289 final, fq. 6. <26file:///C:/Users/pc/Downloads/Albania-Report-2021%20(7).pdf>, aksesuar me 16 korrik 2022

14 Siri Gloppen, 'Courts, corruption and judicial independence' in Tina Søreide and Aled Williams (eds) *Corruption, Grabbing and Development Real World Challenges* (Edward Elgar Publishing 2013) fq. 69.

që jep një vendim të padrejtë në favor të palës që paguan një shumë të hollash (*mitë)*. Megjithatë, sot korrupsioni në gjyqësor, në aspektin juridik shihet në një optikë më të zgjeruar. Ai përfshin sjellje të pandershme, mashtruese ose joetike nga një gjyqtar me qëllim që të ketë përfitime personale ose përfitime për palët e treta.[15] Aktet korruptive përfshijnë të gjitha format e ndikimit të papërshtatshëm që mund të dëmtojnë paanshmërinë e gjyqtarit. të cilat mund të vijnë përveçse nga palët në proces, edhe nga çdo aktor brenda sistemit të drejtësisë, apo dhe jashtë tij.[16] Po ashtu përfitimet e marra apo të premtuara, për vetë apo për të tretë mund të jenë përfitime materiale, politike, avancim në karrierë, apo shmangie e një diçkaje të padëshiruar.[17] Për këtë arsye, në mënyrë që të parandalohet korrupsioni në gjyqësor duhet: (i) të forcohet integriteti i gjyqtarëve me qëllim rritjen e frymës së respektit ndaj ligjit, (ii) të garantohet paanësia në vendimmarrje, si dhe (iii) të konsolidohet pavarësia me qëllim shmangien e çdo ndikimi të paligjshëm politik, apo në nivel hierarkik brenda vetë sistemit gjyqësor.

Në këtë qasje shkon edhe legjislacioni shqiptar,[18] i cili e lidh përfitimin që mund të vijë nga korrupsioni me çdo *"përfitim të parregullt për vete ose për persona të tjerë*", pa u kufizuar tek përfitimet material, apo përfitimi ngushtësisht personal. Ndërkohë nënkuptohet që çdo ndërhyrje në formë "*premtimi, propozimi apo dhënie përfitimi të parregullt*", që mund t'i bëhet gjyqtarit, me qëllim *"për të kryer ose mos kryer një veprim, që lidhet me detyrën a funksionin e tij"* mund të vijë nga çdo person dhe jo detyrimisht nga palët në proces.[19]

Për këtë arsye, kur flasim për parandalim të korrupsionit në gjyqësorin shqiptar do i referohemi parandalimit të ndërhyrjeve, si nga palët ashtu dhe nga individë të tjerë që mund t'i përkasin pushteteve të tjera apo dhe vetë sistemit të drejtësisë. Në këtë këndvështrim është e rëndësishme që të forcohen garancitë që kontribojnë në pavarësinë, paanësine dhe integritetin e

15 Consultative Council of European Judges, 'Preventing Corruption among Judges' (CCJE(2018)3Rev) <https://rm.coe.int/ccje-2018-3e-avis-21-ccje-2018-prevent-corruption-amongst-judges/16808fd8dd> aksesuar më 16 korrik 2022, fq 2-3.

16 Siri Gloppen, 'Courts, corruption and judicial independence' in Tina Søreide and Aled Williams (eds) *Corruption, Grabbing and Development Real World Challenges* (Edward Elgar Publishing 2013) fq. 69.

17 Po aty.

18 Ligji 7895/1995, "Kodi Penal i Republikës së Shqipërisë" [1995] Fletore Zyrtare 2 ndryshuar së fundmi me ligjin 24/2021, "Shfuqizimi i togfjalëshit ´'pa marrë më parë lejen nga organi kompetent sipas dispozitave të vecanta´ në paragrafin e parë të nenit 262 të Kodit Penal të Republikës së Shqipërisë, si i papajtueshëm me nenet 17, pika 1 dhe 47 të Kushtetutës së Republikës së Shqipërisë" Fletore Zyrtare 87 (Kodi Penal i Shqipërisë), nenet 319 dhe 319/ç.

19 Kodi Penal i Republikës së Shqipërisë, nenet 319 dhe 319/ç.

gjyqësorit. Përveç garancive formale ligjore, është e rëndësishme gjithashtu dhe fitimi i besimit të publikut tek paanësia e gjyqësorit, duke përdorur mekanizma që promovojnë transparencën, llogaridhënien dhe përfshirjen e publikut në veprimtritë dhe procedurat që lidhen me gjyqsorin.

3. Shkaqet që kanë kontribur në nivelin e korrupsionit të gjyqësorit në Shqipëri

Për një lufte efektive të korrupsionit dhe sidomos për ta parandaluar atë është e rëndësishme që të njihen shkaqet që çojnë në këtë fenomen. Çdo shoqëri ka specifikat e veta, dhe për pasojë edhe shkaqet që çojnë në korrupsion kanë karakteristika të veçanta, të cilat ndikohet nga konteksti historik, zhvillimet politike, shkalla e zhvillimit ekonomik e kulturor, shkalla e konsolidimit të parimeve të shtetit të së drejtës, cilësia e legjislacionit dhe niveli i zbatimit të tij, etj. Në vijim, do të përmendim disa nga shkaqet që mendohet që kanë çuar në nivelin e lartë të korrupsionit në gjyqësorin shqiptar, përgjatë 30 viteve pas rënies së komunizmit, pa pretenduar të jemi shterrues.

Së pari, *sasia e buxhetit të shtetit dedikuar për sistemin gjyqësor e atë të drejtësisë në përgjithësi, si dhe niveli i ulët i pagave të gjyqtarëve*. Analiza e sistemit të drejtësisë, e bërë para implementimit të reformës, vlerësoi se sistemi i pagave, shpërblimeve, kujdesit social e shëndetësor të gjyqtarëve, si një nga mjetet për garantimin e pavarësisë dhe paanshmërisë së tyre në detyrë, nuk përmbushte standardet e një trajtimi financiar të përshtatashëm dhe dinjitoz të tyre.[20] Për vite me radhë, buxheti i akorduar për sistemin e drejtësisë ka qenë ndër më të paktit në vendet anëtare të Këshillit të Evropës,[21] ndërkohë që pagat kanë qenë ndër më të ultat në Evropë.[22]

Reformimi i sistemit të drejtësisë, i cili po implementohet në Shqipëri të paktën që prej vitit 2016, kishte synim primar luftimin e korrupsionit dhe rikthimin e besimit të publikut tek drejtësia. Për këtë arsye, ndër masat e marra është pikërisht rritja e buxhetit të dedikuar sistemit të drejtësisë dhe

20 Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' *op.cit.*, fq. 75.

21 Sipas raportit të vlerësimit te vitit 2012 kryer nga Komisioni Evropian për Eficiencën e Drejtësisë (CEPEJ) gjykatave dhe prokurorisë shqiptare u janë alokuar 6.1 Euro për frymë, në një kohë që mesatarja e Këshillit të Evropës është 42 Euro për frymë. Shih Nils Muižnieks, 'Në vijim të vizitës në Shqipëri nga 23 deri 27 shtator 2013' (CommDH(2014)1)<https://rm.coe.int/raport-nga-nils-muiznieks-komisioneri-per-te-drejtat-e-njeriut-i-keshi/16806db6cb> aksesuar më 25 qershor 2022, fq 5.

22 Po aty, fq 7.

nivelit të pagave të këtij sektori. Vetëm prej vitit 2019 sistemit gjyqësor iu rritën pagat me mbi dyfishin e atyre ekzistuese, duke i sjellë në një nivel të pranueshëm në raport me rëndësinë e punës që kryen gjyqtari dhe përgjegjësinë që mbart funksioni.[23] Buxheti i miratuar nga ekzekutivi dhe legjislativi, 5 vite pas implementimit të reformës, është në nivelin 89% e buxhetit të kërkuar nga Këshilli i Lartë Gjyqësor (KLGJ), ku pjesa kryesore e tij i dedikohet shpenzimeve për paga.[24]

Së dyti, *mungesa e meritokracisë në emerimin, ngritjen në detyre dhe transferimin e gjyqtarëve.* Për shumë vite, mungesa e transparencës në vendimmarrje, si dhe mosarsyetimi i vendimeve mbi bazën e të cilave bëhen emërimet në detyrë të gjyqtarëve, kanë krijuar bindjen se ato nuk bazohen në meritë apo sistem karriere.[25] Para reformimit të sistemit të drejtësisë qytetarët kane pasur bindjen se emërimi, promovimi në karrierë dhe transferimi bëhej mbi baza lidhjesh politike dhe klienteliste. Për këtë arsye, reforma këto procese sot i la në kompetencë të Këshillit të Lartë të Gjyqësorit, përbërja e së cilit garanton më tepër pavarësi ndaj pushteteve të tjera dhe ushtrimi i funksioneve bëhet mbi baza transparente dhe llogaridhënieje në vendimmarrje.[26]

Së treti, *ndikimi i pushteteve të tjera në veprimtarinë e organit administrues së gjyqësorit*. Para implementimit të reformës në drejtësi, megjithëse legjislacioni garantonte formalisht pavarësinë e gjyqësorit, në realitet janë vërejtur për një kohë të gjatë probleme lidhur me pavarësinë dhe ndikimin e politikës në veprimtarinë e tij. Këshilli i Lartë i Drejtësisë (KLD), i cili ishte përgjegjës për emërimet, ngritjet në detyrë, transferimet, vlerësimin profesional, si dhe procedimet disiplinore ndaj gjyqtarëve të gjykatave të shkallës së parë dhe të apelit, nuk gëzonte besimin e publikut.[27]

23 Ligji 96/2016, "Për Statusin e Gjyqtarëve dhe Prokurorëve në Republikën e Shqipërisë" [2016] Fletore Zyrtare 208 ndryshuar së fundmi me Ligjin 50/2021, "Për disa shtesa dhe ndryshime në ligjin nr. 96/2016 "Për statusin e gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë" [2021] Fletore Zyrtare 71, neni 12.

24 Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' <http://klgj.al/wp-content/uploads/2022/04/RAPORT-VJETOR-2021.pdf> aksesuar më 15 korrik 2022, fq 100.

25 Bazuar në Dokumentin e Analizës së Sistemit të Drejtësisë, në legjislacionin e para reformës "*mungonin detyrime të tjera të qarta për arsyetimin e vendimeve, ofrimin e informacionit dhe raportimin mbi funksionin e organit për të siguruar perceptimin e saktë të publikut lidhur me administrimin e drejtësisë".* Shih për më tepër: Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' *op.cit.*, fq. 59.

26 Ligji 115/2016, "Për Organet e Qeverisjes së Sistemit të Drejtësisë" [2016] Fletore Zyrtare 231 ndryshuar, shih për më tepër seksionin II të Kreut 1 dhe Seksionin II të Kreut II të ligjit.

27 KLD-ja kishte në përbërje të vet 15 anëtarë. Ajo kryhesohej nga Presidenti dhe kishte në përbërje

Prezenca e Presidentit të Republikës dhe Ministrit të Drejtësisë në përbërje të KLD, mundësonte ndikimin e pushteteve të tjera. Nga ana tjetër, zgjedhja e antarëve nga gjyqësori në KLD, pa kritere formale të parashikuara, me miratimin e një shumice të thjeshtë parlamentare, (36 vota nga 140), krijonte mjaftueshëm mungesë besimi mbi pavarësinë nga politika të këtij organi.[28]

Nga ana tjetër, procedimi disiplinor ka qenë një procedurë e paqartë, e cila mbivendoste kompetencat e inspektoratit të Ministrit të Drejtësisë dhe atij të KLD-së, gjë që është parë me shqetësim edhe nga Komisioni i Venecias.[29] Në bazë të ligjit të kohës, vetëm Ministri i Drejtësisë kishte përgjegjësinë për të filluar procedimin disiplinor ndaj gjyqtarëve dhe në cilësinë e anëtarit të KLD-së, edhe pse pa të drejtë vote, merrte pjesë në procedimet disiplinore duke propozuar masa disiplinore.[30] Kjo ishte arsyeja e krijimit të Këshillit të Lartë Gjyqësor (KLGJ) si institucion për qeverisjen e gjyqësorit, me një përbërje dhe përzgjedhje që garanton më tepër pavarësi nga politika, si dhe të nje institucioni te posaçëm dhe të pavarur si Inspektori i Lartë i Drejtësisë, përgjegjës për hetimin dhe propozimin e fillimit të procesit disiplinor.

Së katërti, *ekzistenca e një sistemi inefektiv të vlerësimit etik dhe profesional të gjyqtarëve, i cili kontribuoi në forcimin e kulturës së mungesës së llogaridhënies së sistemit*.[31] Vlerësimi profesional i bërë nga Këshilli i Lartë i Drejtësisë, përveçse i paplotë dhe i cunguar është parë si një proces

---

Kryetarin e Gjykatës së Lartë, Ministrin e Drejtësisë, tre anëtarë të zgjedhur nga parlamenti dhe nëntë gjyqtarë nga 3 shkallët e gjyqësori, të zgjedhur nga Konferenca Kombëtare e Gjyqësorit. Shih për më tepër Ligjin 8811/2001 "Për organizimin dhe funksionimin e Këshillit të Lartë të Drejtësisë" [2001] Fletore Zyrtare 9 i ndryshuar (shfuqizuar).

28 Ligji 8417/1998, "Kushtetuta e Republikës së Shqipërisë" [1998] Fletore Zyrtare 28 ndryshuar së fundmi me Ligjin 16/2022 (Kushtetuta e Republikës së Shqipërisë). Neni 147 i Kushtetutës, para ndryshimeve të reformës (2016) nuk siguronte as formalisht pavarësi politike. Në të nuk parashikoheshin kritere mbi përzgjedhjen e anëtarëve të KLD-së që zgjidhen nga Kuvendi, dhe nuk kërkohej një shumicë e cilësuar që të mund të lejonte edhe shprehjen e vullnetit të forcës politike në minorancë, duke i mundësuar forcës qeverisëse të kandidonte dhe përzgjidhte kandidatëve të preferuar.

29 Venice Commission, 'Judicial Appointments: Report adopted by the Venice Commission at its 70th Plenary Session' (16-17 March 2007, CDL-AD(2007)028) <https://www.venice.coe.int/webforms/documents/CDL-AD(2007)028.aspx> aksesuar më 01 korrik 2022, para 33.

30 Shih Ligjin 8811/2001 "Për organizimin dhe funksionimin e Këshillit të Lartë të Drejtësisë" [2001] Fletore Zyrtare 9 i ndryshuar (shfuqizuar) dhe Ligjin 8678/2001, "Për organizimin dhe funksionimin e Ministrisë së Drejtësisë" [2001] Fletore Zyrtare 27 ndryshuar së fundmi me Ligjin 40/2017 [2017] Fletore Zyrtare 85.

31 Ligji i kohës kishte një vakum ligjor sa i takon kritereve dhe procedurave për vlerësimin profesional të gjyqtarëve. Si bazë për këtë process shërbente vendimi i KLD nr. 261/2, datë 14.04.2010 "Për sistemin e vlerësimit të gjyqtarëve", i cili bazohej në kritere si: aftësia profesionale dhe organizative, aftësia teknike, si dhe aftësia njerëzore/etike.

formal.[32] Një ndër komponentët e vlerësimit profesional, bazohej në numrin e vendimeve që prisheshin nga gjykatat e shkallëve më të larta. Kjo çonte në tejzgjatjen dhe zvarritjen e vlerësimit, sa kohë që vetë zgjidhja e çështjeve në të tre shkallët merrte një kohë relativisht të gjatë.[33] Nga ana tjetër kjo bëntë që vlerësimi profesional të përfshinte periudha që i përkisnin një kohe relativisht të largët nga koha e vlerësimit, ku në shumë raste ndodhte që një pjesë e gjyqtarëve të mos ishin më pjesë e sistemit, për shkak të daljes në pension apo largimit nga gjyqësori.[34] Sot legjislacioni ne fuqi ka rregulla strikte mbi vlerësimin profesional, duke vendosur detyrimin e KLGJ-së për plotësimin e bazës ligjore dhe zhvillimin e këtij procesi[35].

Së pesti, *mungesa e efiçencës së sistemit gjyqësor*. Efiçenca ka qenë dhe vazhdon të mbetet një ndër problemet më të mëdha me të cilat përballet gjyqësori në Shqipëri, edhe pse kemi hyrë në vitin e 6 të aplikimit të reformës në sistemin e drejtësisë. Ngarkesat e gjyqtarëve dhe *backlog-u* i akumuluar prej vitesh tashmë në gjykatat shqiptare, kanë sjellë si pasojë zgjatjen e afateve të gjykimit, duke përbërë një ndër pikat më kritike të sistemit gjyqësor. Shumica e ankesave të qytetarëve ndaj gjyqësorit, në institucionet kompetente vendas (ish KLD, Avokati i Popullit, etj) dhe Gjykata Evropiane e të Drejtave të Njeriut ka të bëjnë me tejzgjatjen e proceseve gjyqësore.[36]

Sot me aplikimin e procesit të rivlerësimit kalimtar (*Vetting*), sistemi operon me mungesa të theksuara në organikë,[37] të cilat kanë sjellë një rritje të metejshme të *backolgut* të akumuluar para reformës[38] dhe rritje të

32 Deri para aplikimit të Reformës në Drejtësi nuk kishte ndonjë gjyqtar të larguar nga detyra për paaftësi. Ndërkohë nga analizimi i vendimeve të Gjykatës së Lartë vërehet një shkallë e lartë e prishjes së vendimeve të shkallëve më të ulta.

33 Nils Muižnieks, 'Në vijim të vizitës në Shqipëri nga 23 deri 27 shtator' *op.cit.*, fq 8.

34 Po aty.

35 Shih per me teper ligjin Nr. 96/2016 "Për Statusin e Gjyqtarëve dhe Prokurorëve në Republikën e Shqipërisë" [2016], i ndryshuar

36 Dokumenti " Analiza e sistemit të drejtësisë në Shqipëri" konstaton se "*deri në shtator të vitit 2014, 70% e ankesave ndaj gjyqtarëve drejtuar KLD i referoheshin zvarritjes së proceseve gjyqësore. Me këtë objekt ishin edhe ankesat e drejtuara Avokatit të Popullit, si dhe ato të depozituara pranë Gjykatës Europiane për të Drejtat e Njeriut, ku deri në këtë vit ishin depozituar rreth 50 çështje kundër Shqipërisë me objekt zvarritjen e gjykimit*." Shih për më tepër Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' *op.cit.*, fq. 103.

37 Gjykatat e shkallës së parë, juridiksioni i përgjithshëm, kanë funksionuar me 70% të gjyqtarëve, ndërsa në juridiksionin administrtiv të shkallës së parë administrative është kryer nga 87.4% e gjyqtarëve të parashikuar. Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq. 79; 89.

38 Sipas Raportit Vjetor të KLGJ për vitin 2021 *"... deri në fund të vitit 2021 në gjykatat e shkallës së parë, juridiksioni i përgjithshëm, stoku është rritur me 7 925 çështje dhe mbeten në pritje*

ngarkesës së gjyqësorit.[39] Deri me tani, janë shkarkuar rreth 220 gjyqtare dhe prokurore, janë dorehequr 79, ndërkohë që janë konfirmuar në detyrë 183 gjyqtare dhe prokurore.[40]

Së gjashti, *mungesa e eficencës dhe transparencës në kontrollin dhe vlerësimin e pasurive të gjyqtarëve*. Një ndër synimet e reformës në drejtësi ishte pastrimi i sistemit gjyqësor nga individë të korruptuar, të cilët do të duheshin t'i nënshtroheshin procesit të *Vetting*-ut, nëpërmjet vlerësimit në tre kritere: pasurisë, profesionalizmit dhe figures.[41] Edhe pse gjyqtarët kanë qenë subjekt i deklarimit të pasurive dhe interesave private që prej vitit 2003,[42] procesi i *Vetting-ut* tregoi se sistemi i kontrollit nuk ka qenë efektiv, sa kohë rreth 62% e gjyqtarëvë dhe prokurorëve të vettuar nuk kaluan këtë proces kryesisht pasi nuk kaluan testin e pasurisë, duke mos justifikuar me burime të ligjshme pasuritë e deklaruara.[43]

Së shtati, *mungesa e transparensës në vendimmarrjet e gjyqësorit*. Gjyqësori për një kohë të gjatë ka vuajtur nga mungesa e infrastrukturës fizike, niveli i ulët të përdorimit të teknologjisë së informacionit, apo kushtet e papaërshtatshme të punës së gjyqtarëve. Shumica e seancave gjyqësore, civile dhe administrative, janë zhvilluar në zyrat e gjyqtarëve, për shkak të numrit të kufizuar të sallave të gjykimit nëpër gjykata. Procesverbalet e seancës mbaheshin me shkrim nga sekretaret,[44] ndërkohë që sistemi audio, është implementuar relativisht vonë dhe nuk ka funksionuar njëkohësisht në të gjitha gjykatat e vendit.[45] Palët merrnin informacion për datat dhe

---

të gjykimit 36 579 çështje…. Numri i çështjeve të pashqyrtuara në gjykatat administrative të shkallës së parë (backlog-u) në fund të vitit 2021, u rrit me 12%, duke shënuar një total prej 6278 çështje në pritje për t'u gjykuar." Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq 79; 89.

39 Referuar Raportit Vjetor 2021 të KLGJ : "*…në gjykatat administrative të shkallës së pare ka pasur një rritje të ngarkesës mesatare të gjyqtarëve në 785.07 çështje për gjyqtar, krahasuar me 593.5 çështje/gjyqtar në vitin 2020"*

40 Reporter.al, 'Ecuria e Vetingut' (3 gusht 2022) <https://reporter.al/vetingu/> aksesuar më 3 gusht 2022.

41 Shih nenin 4, pika 1 të Ligjit Nr. 84/2016 "Për rivlerësimin kalimtar të gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë", i ndryshuar

42 Ky proces bazohej në ligjin Nr .9049, date 10.4.2003 "Per deklarimin dhe kontrollin e pasurive, te detyrimeve financiare te te zgjedhurve dhe te disa nepunesve publike", i ndryshuar

43 Commission, 'Key findings of the 2021 Report on Albania' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_5276> aksesuar më 07 korrik 2022.

44 Kjo praktikë është përdorur deri në 2013, me miratimin e Ligjit 122/2013, "Për disa shtesa dhe ndryshime në ligjin nr. 8116, datë 29.03.1996 "Kodi i Procedurës Civile i Republikës së Shqipërisë" [2013] Fletore Zyrtare 180 ndryshuar.

45 Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' *op.cit.*, fq. 77.

oraret e seancave gjyqësore në Gjykatën e Apelit dhe Gjykatën e Lartë vetëm nëpërmjet afishimit të bërë pranë godinave të gjykatës. Ndërkohë që, megjithëse garantohej ligjërisht që vendimet duhet të shpallën publikisht, ka vështirësi në aksesimin e vendimeve të arsyetuara, për shkak të ngarkesës së gjyqtarëve, si dhe vështirësive në anonimizimin e të dhënave personale të shfaqura në vendime. Mungesa e transparencës e shkaktuar nga aksesi i kufizuar në informacion në lidhje me sistemin gjyqësor, lehtëson sjelljen korruptive dhe për këtë arsye shpesh është një shkas i rëndësishëm për korrupsion.[46] Për këtë, Reforma në Drejtësi e vuri theksin tek operimi i KLGJ-së mbi baza transparence[47].

Së fundmi, *niveli i ulët i ndëshkueshmërisë së korrupsionit në rradhët e gjyqësorit*. Edhe pse prej vitesh gjyqësori shihet si një ndër sektorët me korrupsion të lartë, numri i gjyqtarëve të dënuar për korrupsion mbetet tejet i ulët. Shkaqet variojnë që nga kultura e pandërshkueshmërisë që ka mbizotëruar për një kohë të gjatë për veprat e korrupsionit në përgjithësi, tek imuniteti i gjerë i gjyqtarëve, i keqpërdor në funksion të mosdënimit të tyre.[48] Këtij qëllimi i shërben ngritja e strukturave të posacme me qëllim hetimin dhe gjykimin e korrupsionit dhe krimit të organizuar, si Prokurorisë së Posaçme kundër Korrupsionit dhe Krimit të Organizuar, Byrosë Kombëtare të Hetimit/Njësisë së Posaçme Hetimore, si dhe Gjykatës së Shkallës së Parë dhe të Apelit për Krimin e Organizuar dhe Korrupsionin[49]

4. Reformimi i sistemit të drejtësisë në Shqipëri

Parandalimi i korrupsionit në sistemin gjyqësor, kërkon vullnet politik dhe burime financiare me qëllim marrjen e masave ligjore, organizative dhe infrastrukturore, të cilat ndikojnë në një sistem të pavarur dhe të paanshëm. Modelet e suksesshme për luftimin e korrupsionit në gjyqësor vijnë nga shtetet në të cilat sistemi gjyqësor karakterizohet nga niveli i lartë i integritetit,

46 Consultative Council of European Judges, 'Preventing Corruption among Judges' (CCJE(2018)3Rev) <https://rm.coe.int/ccje-2018-3e-avis-21-ccje-2018-prevent-corruption-amongst-judges/16808fd8dd> aksesuar më 16 korrik 2022, fq 3.

47 Shih nenin 2 të ligjit 115/2016, "Për Organet e Qeverisjes së Sistemit të Drejtësisë" [2016] Fletore Zyrtare 231 ndryshuar

48 Sipas raportit të Komisionerit për të Drejtat e Njeriut i Këshillit të Evropës Nils Muižniek: "*UNHRC ka konstatusr si pengesë serioze për një ndjekje penale të efektshme të rasteve të korrupsionit imunitetin e gjerë nga ndjekja penale që gëzonin zyrtarët e shtetit, përfshirë edhe anëtarët e gjyqësorit"*. Nils Muižnieks, 'Në vijim të vizitës në Shqipëri nga 23 deri 27 shtator 2013' *op.cit.*, fq 6.

49 Shih ligjin nr. 95/2016 "Për organizimin dhe funksionimin e institucioneve për të luftuar korrupsionin dhe krimin e organizuar"

llogaridhënies, transparencës, eficencës dhe pjesëmarrjes së publikut.[50]

Aktualisht sistemi i gjyqësorit në Shqipëri po i nënshtrohet një reformimi të thellë. Reforma, e cila ka filluar implementimin prej vitit 2016 synonte: (i) së pari, pastrimin e gjyqësorit nga rradhët e të korruptuarve, nëpërmjet aplikimit të proçesit të *Vetting*-ut dhe ii) së dyti, riorganizimin e sistemit të drejtësisë duke ndryshuar konceptimin e strukturës qeverisëse të tij, në mënyrë që të rritet eficenca, profesionalizmi, si dhe të forcohen garancitë ligjore që kontribojnë në pavarësisë, paanësisë, dhe integritetit brenda sistemit gjyqësor.[51]

Në funksion të sa më sipër, hapi i parë ishte ndërmarrja e një reformë legjislative e cila preku dispozitat kushtetuese dhe ato të ligjeve organike që rregullonin qeverisjen e gjyqësorit, organizimin, funksionimin, statusin e gjyqtarëve, etj.[52] Këto ndryshime sollën: i) krijimin e strukturave të reja të qeverisjes së gjyqësorit, duke garantuar pavarësi nga ndikimi politik në përbërjen dhe përzgjedhjen e antarëve të tyre; ii) pavarësi në proçesin disiplinor të gjyqtarëve, nëpërmjet krijimit të rregullave strikte dhe një strukture të posaçme si Inspektori i Lartë i Drejtësisë; iii) uljen e ndikimit të pushteteve të tjera në përzgjedhjen e gjyqtarëve në përbërje të Gjykatës së Lartë dhe Gjykatës Kushtetuese; iv) konsolidimin e statusit të gjyqtarëve, etj.[53] Ndryshimet përbëjnë garanci, të paktën në nivel ligji, të forcimit të

50 James Michel, 'Reducing Corruption In The Judiciary' (Office of Democracy and Governance USAID Program Brief 2009) <https://pdf.usaid.gov/pdf_docs/Pnadq106.pdf> aksesuar 07 korrik 2022, fq 4.

51 Grupi i Ekspertëve të Nivelit të Lartë, 'Strategjia e Reformës në Sistemin e Drejtësisë' (24 korrik 2015) <https://rm.coe.int/strategjia-ne-refomen-e-sistemit-te-drejtesise/16809eb53a,aksesuar> aksesuar më 07 korrik 2022, fq 2.

52 Reformimi i sistemit të drejtësisë përfshiu, ndër të tjera, ndryshime në Ligjin 8417/1998, "Kushtetuta e Republikës së Shqipërisë" [1998] Fletore Zyrtare 28 ndryshuar së fundmi me Ligjin 16/2022 (Kushtetuta e Republikës së Shqipërisë); Ligjin 9877/2008 "Për organizimin e pushtetit gjyqësor në Republikën e Shqipërisë" [2008] (shfuqëzuar); Ligji 49/2012, "Për organizimin dhe funksionimin e gjykatave administrative dhe gjykimin e mosmarrëveshjeve administrative" [2012] Fletore Zyrtare 49 (i ndryshuar); Ligji 8811/2001, "Për organizimin dhe funksionimin e Këshillit të Lartë të Drejtësisë" [2001] Fletore Zyrtare 9 (shfuqizuar); Ligji 9049/2003, "Për deklarimin dhe kontrollin e pasurive, të detyrimeve financiare të të zgjedhurve dhe të disa nëpunësve publikë" [2003] Fletore Zyrtare 31 ndryshuar me Ligjin 105/2018; Ligji 9367/2005, "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike" [2005] Fletore Zyrtare 31 ndryshuar me Ligjin 44/2014; Ligji 8136/1996, "Për Shkollën e Magjistraturës" [1996] Fletore Zyrtare 21 (shfuqëzuar); Ligji 8678/2001, "Për organizimin dhe funksionimin e Ministrisë së Drejtësisë" [2001] Fletore Zyrtare 27, ndryshuar së fundmi me Ligjin 40/2017 [2017] Fletore Zyrtare 85.

53 Ligji 115/2016, "Për Organet e Qeverisjes së Sistemit të Drejtësisë" [2016] Fletore Zyrtare 231 ndryshuar; Ligji 177/2014, "Për disa shtesa dhe ndryshime në ligjin nr. 8588, datë 15.3.2000, "Për organizimin dhe funksionimin e Gjykatës së Lartë të Republikës së Shqipërisë" [2014] Fletore Zyrtare 217 me të cilin u ndryshua Ligji 8588/2000, "Për organizimin dhe funksionimin

pavarësisë, paanësisë dhe integritetit e profesionalizmit. Në këtë kontekst, këto masa pritet të minimizojnë edhe efektin e faktorëve kriminogjenë të cilët ndikojnë në korrupsionin e sistemit gjyqësor, të përmendur më sipër.

Sot, pas 5 vitesh implementimi, është ende në proces *Vetting*-u i gjyqtarëve dhe janë në fazë konsolidimi institucionet e reja të prodhura prej Reformës, si Këshilli i Lartë Gjyqësor, Inspektorati i Lartë i Drejtësisë, SPAK, etj. KLGJ, në cilësinë e organit themelor në qeverisjen e gjyqësorit ka adresuar problemet më emergjente të sistemit, që lidhen me funksionalitetin e Gjykatës Kushtetuese dhe Gjykatës së Lartë, veprimtaria e të cilave u pezullua për rreth dy vite për shkak të largimit nga sistemi të gjyqtarëve të këtyre gjykatave, si dhe me miratimin e hartës së re gjyqësore që riorganizon gjykatat e shkallës së parë dhe apelit, me qëllim rritjen e eficencës së tyre.[54]

5. Teknologjia e Informacionit në gjykata dhe parandalimi i korrupsionit në gjyqësor

Buxheti i akorduar në këtë drejtim ka qenë në nivele të krahasueshme me vendet e tjera tw KiE, të të njëjtit grup (Bosnje Hercegovinën, Gjeorgjinë dhe Moldavinë), por kjo vlerë pwrswri mbetet poshtw vlerave mesatare dhe mediane evropiane (3,1 dhe 3,8%)[55]. Nga ana tjetwr, autoritetet gjyqësore për një periudhë të gjatë kohë nuk ishin të përgatitura për ta shfrytëzuar këtë sistem[56]. Masat e marra pjesërisht, mungesa e trajnimeve tw stafit, si dhe mungesa e vullnetit ka bërë që këto masa të mos kenë impaktin e pritur, si në efiçencë ashtu edhe në parandalimin e korrupsionit. Për këtë arsye, ndër masat që do të jetëzonin synimet e refomës për rritjen e pavarësisë, efiçiencës dhe profesionalizmit në gjyqësor, kishin të bënin me rritjen e përdorimit të teknologjisë së informacionit dhe dixhitalizimin e një sërë proceseve që lidhen me veprimtarinë e përditshme të gjykatave.[57] Hapi i

---

e Gjykatës së Lartë të Republikës së Shqipërisë" [2000] FZ 7; Ligji 8577/2000, "Për organizimin dhe funksionimin e Gjykatës Kushtetuese të Republikës së Shqipërisë" [2000] FZ 4 ndryshuar me Ligjin 99/2016.

54 Këshilli i Lartë Gjyqësor, 'Relacion mbi Projekt-Aktin "Për Miratimin e Raportit Vlerësues dhe Propozimit të Grupit Ndërinstitucional të Punës mbi Riorganizimin e Rretheve Gjyqësore dhe Kompetencave Tokësore të Gjykatave" <http://klgj.al/ëp-content/uploads/2022/06/relacion-harta-gjyqesore-F-1-Mbledhje-Plenare.pdf> aksesuar më 3 gusht 2022.

55 Jacques Bühler dhe Jon Johnsen, 'Raporti i Vlerësimit në Thellësi të Sistemit të Drejtësisë në Shqipëri' (2015)<https://rm.coe.int/mbeshtetje-e-be-kie-per-efikasitetin-e-drejtesise-sej-nje-projekt-i-pe/1680788436> aksesuar me 13 korrik 2022, fq 11.

56 Po aty.

57 Strategjia e Reformës në Sistemin e Drejtësisë synonte ".. *modernizimin e sistemit përmes*

parë që do i shërbentë implementimit të masave që lidhen me teknologjinë e informacionit ishte ngritja e Qendrës së Teknologjisë së Informacionit për Sistemin e Drejtësisë (QTI), si organ rregullator dhe përcaktues i standardeve në fushën e teknologjisë së informacionit për të gjithë sistemin e drejtësisë.[58] Në vijim, për qëllim të këtij artikulli, do të ndalemi tek disa nga proceset ku perfshirja e teknologjise se informacionit mundeson rritjen e pavaresise, transparencën, llogaridhënien dhe aksesin e publikut në gjykata, parakushte këto në parandalimin e korrupsionit.

Emërimi i gjyqtarëve në pozicionin e punës mbi baza merite është kushti themelor për një gjyqësor të pavarur dhe me integritet. Për këtë arsye, transparenca e kushteve dhe kritereve të emërimit në detyrë dhe procedurat e hapura të emërimit, ngritjes në detyrë apo transferimit të gjyqatarëve janë një garanci që në pozicionin e gjyqtarëve do të jenë persona profesionistë dhe të pavarur. GRECO në Raundin e Katërt të Vlerësimit për Shqipërinë në një ndër Rekomndimet vinte theksin në transparencën e përzgjedhjes së antarëve të Gjykatës së Lartë.[59] Aktualisht zgjedhja, promovimi, qendrimi ne detyre dhe transferimi i gjyqtarëve të të tre shkallëve bazohen ne procedura transparente. Aktet qe rregullojne kriteret e mësipërme jane lehtesisht te aksesueshme në fazën ëeb,[60] ndërkohë që mbledhjet plenare të KLGJ-së mund te aksesohen në kohë reale *online* nga personat e interesuar dhe aktorë të ndryshem nëpërmjet platformës *Zoom*. Regjistrimi audio dhe procesverbali me përmbledhjen e diskutimeve të mbledhjeve publikohet në faqen zyrtre të KLGJ-së.[61]

---

zbatimit të teknologjive të reja, me vëmendje të posaçme ndaj vendosjes së teknologjisë së informacionit në çdo zyrë dhe në çdo proces të hetimit e gjykimit, vendosjen e komunikimit online të institucioneve të sistemit, forcimin e sistemit të mbrojtjes së të dhënave, realizimin e një arkivi unik kombëtar të vendimeve gjyqësore, krijimin e një regjistri të unifikuar kombëtar statistikor me të dhënat e sistemit" etj. Shih për më tepër Grupi i Ekspertëve të Nivelit të Lartë, 'Strategjia e Reformës në Sistemin e Drejtësisë' (24 korrik 2015) <https://rm.coe.int/strategjia-ne-refomen-e-sistemit-te-drejtesise/16809eb53a,aksesuar> aksesuar më 07 korrik 2022, fq 50.

58 Vendimi e Këshillit të Ministrave 972/2020, 'Për organizimin, funksionimin e përcaktimin e kompetencave të Qendrës së Teknologjisë së Informacionit për Sistemin e Drejtësisë' [2012] FZ 213. Nëpërmjet këtij vendimi, u ngrit Qendra e Teknologjisë së Informacionit për Sistemin e Drejtësisë (QTI).

59 Shih: GRECO, 'Raundi i Katërt i Vlerësimit - Parandalimi i korrupsionit në lidhje me deputetët, gjyqtarët dhe prokurorët- Shtojcë E Raportit Të Dytë Të Përputhshmërisë Shqipëri' (Greco 2020), fq 7 <https://rm.coe.int/raundi-i-katert-i-vleresimit-parandalimi-i-korrupsionit-ne-lidhje-me-d/16809fd88d, > aksesuar me 5 gusht 2022

60 Shih për më tepër aktet e publikuara në faqen zyrtare të KLGJ-së. Këshilli i Lartë Gjyqësor, 'Vendime' < http://klgj.al/vendime/> aksesuar më 15 korrik 2022.

61 KLGJ, 'Përmbledhja e Diskutimeve: Regjistrimi Audio' <http://klgj.al/dokumentimi-i-mbledhjes-plenare/> aksesuar me 15 korrik 2022.

Një mjet gjerwsisht i pranuar, i cili ndikon në paanësinë e gjyqtarit dhe e imunizon atw nga ndikimi hierarkik është ndarja e çështjeve gjyqësore të regjistruara ndërmjet gjyqtarëve nw mwnyrw rastwsore dhe transparente. Ligji 98/2016 "Për organizimin e pushtetit gjyqësor në Republikën e Shqipërisë" të ndryshuar parashikon që ndarja e çështjeve gjyqësore duhet të bëhet me short, i cili realizohet në rrugë elektronike, bazuar në parimet e transparencës dhe të objektivitetit.[62] Ligji 98/2016 ngarkon më tej Këshillin e Lartë Gjyqësor për miratimin e rregullave më të hollësishme për programin dhe procedurat e ndarjes së çështjeve me short, si dhe Inspektorin e Lartë të Drejtësisë për kryerjen rregullisht të inspektimeve lidhur raportet e sistemit elektronik të paktën një herë në vit.[63] Aktualisht këto garanci ligjore, janë të zbatuara në praktikë. Prej vitesh në gjykatat shqiptare ndarja e çështjeve bëhet me short dhe nëpërmjet aplikacionit "*Kioska*" mundësohet afishimi i shortit elektronik në hollin e gjykatës.[64]

Automatizimi i sistemit të menaxhimit të çështjeve në gjykata shihet si një mjet efektiv i parandalimit të korrupsionit dhe reformat në këtë drejtim kanë rezultuar efektive në funksion të rritjes së transparencës, drejtësisë dhe eficencës.[65] Sistemi i menaxhimit të çështjeve (ICMIS), edhe pse ka mbi një dekadë që është krijuar, nuk ka qenë asnjëherë plotësisht funksional në të gjitha elementët e tij, si dhe nuk përdorej nga të gjitha gjykatat. Edhe pse qëllimi i këtij sistemi ka qenë të lehtësonte punën e gjykatave, mos funksionimi i plotë i tij, ka sjellë si pasojë e kryerjes nga gjykatat të një pune dyfishe.[66] Këto probleme kanë bërë që Këshilli i Lartë Gjyqësor, përgjatë viteve të funksionimit të tij të implementojë rreth 84 ndryshime të rëndësishme në sistemet ICMIS, me qëllim adresimin e problematikave të

62 Ligji 98/2016, "Për organizimin e pushtetit gjyqësor në Republikën e Shqipërisë" [2016] Fletore Zyrtare 209 ndryshuar nga Ligji 46/2021, neni 25.

63 Po aty

64 Një sërë sistememesh elektronike janë zhvilluara në kudër të projekteve të finncuar nga USAID në kuadër të rritjes së efiçencës në gjykata. KLGJ, 'Vendim Nr 47, date 08.02.2022 Për Miratimin e 'Raportit Vjetor mbi Veprimtarinë e Komisionit Komisionit të Planifikimit Strategjik, Administrimit dhe Buxhetit për vitin 2021' <http://klgj.al/ëp-content/uploads/2022/04/RAPORTI-VJETOR-MBI-VEPRIMTARINË-E-KOMISIONIT-TË-PLANIFIKIMIT-STRATEGJIK-ADMINISTRIMIT-DHE-BUXHETIT-PËR-VITIN-2021"-BASHKELIDHUR-VENDIMIT-Nr.47-datë-08.02.2022.pdf> aksesuar më 10 korrik 2022, fq 24.

65 James Michel, 'Reducing Corruption In The Judiciary' (Office of Democracy and Governance USAID Program Brief 2009) <https://pdf.usaid.gov/pdf_docs/Pnadq106.pdf> aksesuar 07 korrik 2022, fq 10.

66 Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2020' <http://klgj.al/ëp-content/uploads/2021/06/Raporti-Vjetor-KLGJ-2020.pdf> aksesuar më 15 korrik 2022, fq 41.

evidentuara për vite nga përdoruesit e këtij sistemi në gjykata[67]. Aktualisht është thjeshtuar përdorimi i sistemit, duke i mundësuar përdoruesit që mbi bazën e aplikacionit "*1-click",* të mund të gjenerojnë me një klikim të vetëm informacion lidhur me dosjen gjyqësore, fletën e shortit, procesverbalet e seancave, listën e planifikimeve dhe të gjitha vendimet e çështjes.[68] Një masë tjetër, e cila shkon në drejtim të parandalimit të klientelizmit dhe korrupsionit, e implementuar së fundmi në këtë sistem është pikërisht mundësia e zgjedhjes së avokatëve kryesisht në mënyrë rastësore.[69]

Përpunimi i statistikave dhe bërja e tyre transparente është e rëndësishme për të vlerësuar eficencën e gjyqësorit dhe për të matur ngarkesën dhe performancën e gjyqtarëve. Vonesat dhe tejzgjatja e çështjeve gjyqësore, mund të ndodhë që të kenë bazë korrupsionin.[70] Për këtë arsye është e rëndësishme që të përpunohen dhe bëhen publike statistika të cilat vlerësojnë performancën e gjyqtarëve, me qëllim vlerësimin e shkaqeve në vonesat e proceseve. Aktualisht këtij qëllimi i shërben përdorimi i sistemit të menaxhimit të çështjeve, edhe si një mundësi për gjenerimin e të dhënave statistikore, sipas formateve të reja, të miratuara së fundmi nga KLGJ.[71]

Aktualisht KLGJ është në proces të ndërtimit të një sistemi të ri të menaxhimit të çështjeve (CMS). Ky sistem do të mundësojë menaxhimin e të dhënave dhe dokumenteve, bazuar në ëeb, për të gjitha gjykatat në Shqipëri dhe do të funksionojë me një instalim të vetëm, të centralizuar, që do të lehtësojë përditësimin e sistemit të menaxhimit të çështjeve me programe të avancuara kompjuterike.[72] Sistemi i ri pritet që të rrisë krahas efiçencës edhe llogaridhënien dhe përfshirjen e përdoruesve të gjykatës nëpërmet: i) sigurimit të aksesimit me një ndalëse të vendimeve gjyqësore; ii) mundësimit të depozitimit elektronik; iii) pagesës elektronike; iv) njoftimeve elektronike; v) aksesin në dosjet dixhitale; si dhe vi) zhvillimin

67 Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq 108

68 Po aty, fq 109.

69 Po aty

70 James Michel, 'Reducing Corruption in the Judiciary' (Office of Democracy and Governance USAID Program Brief 2009) <https://pdf.usaid.gov/pdf_docs/Pnadq106.pdf> aksesuar 07 korrik 2022, fq 11.

71 Raportimi nga ana e gjykatave gjenerohet në mënyrë të automatizuar sipas vendimit të KLGJ nr. 47, datë 11.02.2021 "Për miratimin e "Udhëzuesit për mbajtjen dhe plotësimin e tabelave me të dhëna statistikore për efekt të mbajtjes dhe monitorimit të produktivitetit dhe efiçencës së gjykatave". Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq 113.

72 Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e Këshillit të Lartë Gjyqësor për vitin 2021' *op.cit*, fq 114.

e përdorimit të dosjeve elektronike (sistemi e-filing) nga të gjithë aktorët e sistemit të drejtësisë (si prokuroritë, përmbaruesit, avokatët, etj).[73]

Mungesa e transparencës, e shkaktuar nga aksesi i kufizuar në informacion në lidhje me sistemin gjyqësor, shpesh është një shkas i rëndësishëm për korrupsion.[74] Ndërkohë, është mëse e provuar se një sistem gjyqësor me një shkallë të lartë transparence dhe integriteti paraqet mbrojtjen më të mirë kundër korrupsionit.[75] Në këtë kontekst një rol me rëndësi luan transparenca e proceseve gjyqësore. Në kuadër të rritjes së transparencës dhe llogaridhënies, janë marrë një sërë masash që përfshijnë ose mundësohen nëpërmjet teknologjisë së informacionit. Kështu mund të përmendim:

- kalendarin e menaxhimit të përdorimit të sallave të gjykimit nëpër gjykata, i cili adreson problemin e mbajtjes së seancave gjyqësore në zyrat e gjyqtarëve, që sillte mungesë transprence dhe llogaridhënie;[76]
- pajisjen e sallave me sistemin audio i cili rregjistron seancat dhe nëpërmjet aplikacionit *Backup Chain* mundëson transferimin e regjistrimeve audio nga serverët e gjykatave tek serveri qendror pranë AKSHI-t;[77]
- sistemin elektronik *Kioska* i cili mundëson shfaqjen elektronikisht në hollin e gjykatës të kalendarit të seancave, si dhe informacionet mbi çështjet; dhe[78]
- aksesimin nga palët në proces të informacionit për çështjen dhe vendimet gjyqësore të paanonimizuara, nëpërmjet mënyrës së identifikimit të sigurt.[79]

---

73 Po aty.

74 Consultative Council of European Judges, 'Preventing Corruption among Judges' (CCJE(2018)3Rev) <https://rm.coe.int/ccje-2018-3e-avis-21-ccje-2018-prevent-corruption-amongst-judges/16808fd8dd> aksesuar më 16 korrik 2022, fq 3.

75 Po aty

76 Ky Kalendar mbahet nëpërmjet sistemit elektronik të financuar nga USAID (*Calendar Menagement System PAKS+*), i cili tani gjendet ne pronesi të KLGJ. KLGJ, 'Vendim Nr 47, date 08.02.2022 Për Miratimin e 'Raportit Vjetor mbi Veprimtarinë e Komisionit Komisionit të Planifikimit Strategjik, Administrimit dhe Buxhetit për vitin 2021' <http://klgj.al/ëp-content/uploads/2022/04/RAPORTI-VJETOR-MBI-VEPRIMTARINË-E-KOMISIONIT-TË-PLANIFIKIMIT-STRATEGJIK-ADMINISTRIMIT-DHE-BUXHETIT-PËR-VITIN-2021"-BASHKELIDHUR-VENDIMIT-Nr.47-datë-08.02.2022.pdf> aksesuar më 10 korrik 2022, fq 24.

77 Po aty.

78 Po aty.

79 Të dhënat sigurohen nëpërmjet një ID-je universale unike, duke përdorur një numër pseudo të rastësishëm 128-bit. Shih për më tepër lidhur me përdorimin e të dhënave gjyqësore

Teknologjia e informacionit është përdorur edhe me qëllim aksesin e qytetarëve në gjykatë. Kështu në portalin e përbashkët të gjykatave, ofrohet aplikimi online për shërbimet administrative në gjykatë nëpërmjet implementimit të formularit elektronik të aplikimit.[80] Nëpërmjet këtij aplikacioni qytetari plotëson formularin e aplikimit duke specifikuar shërbimin e kërkuar dhe dokumentacioni (vendime gjyqësore, kopje dosjesh gjyqësore dhe dokumentacion nga arkiva e gjykatës), brenda 48 orëve mund të tërhiqet pranë sporteleve të gjyktës.[81]

Duke qenë se një ndër synimet e reformimit të sistemit të drejtësisë ishte rritja e cilësisë së shërbimit në gjykata dhe besimit të publikut tek drejtësia Ligji 115/2016 "Për organet e qeverisjes së sistemit të drejtësisë" parashikon zhvillimin e vrojtimeve për vlerësimin e shërbimeve të gjykatave nga përdoruesit e tyre.[82] Këtyre vrojtimeve do u vijë në ndihmë, një pyetësor online që mat kënaqësinë e përdoruesve të gjykatës.[83] Pyetësori përveçse do të plotësojë një detyrim ligjor, do përmbushë nevojën e sistemit gjyqësor për të kuptuar cilësinë e shërbimeve të ofruara ndaj qytetarit dhe profesionistëve të drejtësisë.

6. Konkluzione

Shqipëria hyn tek vendet ku perceptimi i nivelit të korrupsionit është i lartë. Një ndër sektorët më të ndjeshëm, ku publiku referon shkallë të lartë korrupsioni për vite ka qenë sistemi i drejtësisë. Kjo ishte arsyeja që nga 2016, sistemi i drejtësisë në tërësi iu nënshtrua një reformimi të thellë, i cili synonte të pastronte sistemin nga gjyqtarët e korruptuar, si dhe të rriste eficencën e gjykatave dhe cilësinë në dhënien e drejtësisë. Për këtë arsye, u morën një sërë masash për ndryshime ligjore, të cilën prekën Kushtetutën dhe gjithë legjislacionin që rregullonte sektorët e drejtësisë. U ndryshua arkitektura e qeverisjes së gjyqësorit dhe prokurorisë, si dhe inspektimi i tyre. Gjithashtu, u morën një sërë masash institucionale të cilat syonin rritjen

të anonimizuara Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq 111.

80 Po aty.

81 Po aty.

82 Ligji 115/2016, "Për Organet e Qeverisjes së Sistemit të Drejtësisë" [2016] Fletore Zyrtare 231 ndryshuar, neni 94, pika 5, shkronja "a".

83 Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' *op.cit.*, fq 113.

e pavarësisë, paanësisë, profesionalizmit dhe integritetit të gjyqësorit.

Megjithëse Reforma në Drejtësi është në vitin e gjashtë të aplikimit të saj, masat institucionale dhe infrastrukturore janë implementuar në mënyrë graduale, pasi një kohë të konsiderueshme mori ngritja e institucioneve dhe bërja e tyre funksionale. Aktualisht institucionet janë në fazë konsolidimi, ku ndërkohë dy vitet e fundit kanë qenë vitet e investimeve në nevojat më emergjente të sistemit, që i referohen kryesisht funksionalitetit të gjykatave, sidomos asaj të Lartë dhe Kushtetuese. Në vëmendje të organit të qeverisjes së gjyqësorit, ka qenë investimi në infrastrukturë, ku një peshë të rëndësishme zënë investimet në fuqizimin e infrastrukturës së teknologjisë së informacionit. Ato i kanë shërbyer sidomos rritjes së transparencës, llogaridhënies dhe hapjes së sistemit gjyqësor ndaj publikut. Këto të fundit pritet që të ndikojnë në mënyrë të drejtpërdrejtë edhe në parandalimin e korrupsionit në gjyqësor.

Edhe pse rezultatat e reformave kanë filluar të ndihen në sistemin e drejtësisë, eshte ende heret per te vleresuar impaktin e plotë që ato do të kenë. Në këtë këndvështrim, edhe pse janë marrë një sërë masash për dixhitalizimin e një sërë proceseve që lidhen me gjyqësorin dhe janë implementuar apo përsosur një sërë sistemesh dhe aplikacionesh, ka pak të dhëna që mundësojnë vlerësimin e impaktit real që ato, së bashku me masa të tjera, do të kenë në parandalimin e korrupsionit në gjyqësor. Megjithatë, ajo që mund të themi në këto moment është se këto masa janë në përputhje dhe duket që shkojnë në të njëjtën linjë me rekomandimet e Greco-s, të CEPEJ, Këshillit të Evropës lidhur me parandalimin e korrupsionit. Ato gjithashtu përkojnë me masat që sot implementohen nga vende që karakterizohen nga një sistem gjyqësor me integritet, nivel të ulët korrupsioni e besim të lartë të qytetarëve tek organet e drejtësisë.

References

Bühler Jacques dhe Johnsen Jon, 'Raporti i Vlerësimit në Thellësi të Sistemit të Drejtësisë në Shqipëri' (2015) <https://rm.coe.int/mbeshtetje-e-be-kie-per-efikasitetin-e-drejtesise-sej-nje-projekt-i-pe/1680788436> aksesuar me 13 korrik 2022

Commission, 'Albania 2021 Report' (Communication) (2021) SËD(2021) 289 final

Commission, 'Key findings of the 2021 Report on Albania' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_5276> aksesuar

më 07 korrik 2022.

Consultative Council of European Judges, 'Preventing Corruption among Judges' (CCJE(2018)3Rev) <https://rm.coe.int/ccje-2018-3e-avis-21-ccje-2018-prevent-corruption-amongst-judges/16808fd8dd> aksesuar më 16 korrik 2022

Council of the European Union, 'Council conclusions on enlargement and stabilisation and association process - Albania and the Republic of North Macedonia' (25 mars 2020) <https://data.consilium.europa.eu/doc/document/ST-7002-2020-INIT/en/pdf> aksesuar më 15 qershor 2022

Departamenti Amerikan i Shtetit, 'Raporti për të Drejtat e Njeriut 2021: Shqipëria' <https://al.usembassy.gov/sq/our-relationship-sq/official-reports-sq/> aksesuar më 15 qershor 2022

DË, 'Lufta kundër korrupsionit është përgjegjësi e vetë qeverive të Ballkanit Perëndimor' <https://www.dw.com/sq/lufta-kundër-korrupsionit-është-përgjegjësi-e-vetë-qeverive-të-ballkanit-perëndimor/a-60553484> aksesuar më 15 qershor 2022

Euronews Albania, '92% e shqiptarëve mendojnë se qeverisja është e zhytur në korrupsion' <https://euronews.al/programs/shqiperi/barometri/2021/09/23/live-l-92-e-shqiptareve-mendojne-se-qeverisja-eshte-e-zhytur-ne-korrupsion/> aksesuar më 15 qershor 2022

Gloppen Siri, 'Courts, corruption and judicial independence' in Tina Søreide and Aled Williams (eds) *Corruption, Grabbing and Development Real World Challenges* (Edward Elgar Publishing 2013)

Grupi i Ekspertëve të Nivelit të Lartë, 'Analizë e Sistemit të Drejtësisë në Shqipëri: dokument i hapur për vlerësime, komente dhe propozime' (qershor 2015) <http://www.reformanedrejtesi.al/sites/default/files/dokumenti_shqip_0.pdf> aksesuar më 15 qershor 2022

Grupi i Ekspertëve të Nivelit të Lartë, 'Strategjia e Reformës në Sistemin e Drejtësisë' (24 korrik 2015) <https://rm.coe.int/strategjia-ne-refomen-e-sistemit-te-drejtesise/16809eb53a,aksesuar> aksesuar më 07 korrik 2022

James Michel, 'Reducing Corruption in The Judiciary' (Office of Democracy and Governance USAID Program Brief 2009) <https://pdf.usaid.gov/pdf_docs/Pnadq106.pdf> aksesuar 07 korrik 2022

Këshilli i Lartë Gjyqësor, 'Vendime' < http://klgj.al/vendime/> aksesuar më 15 korrik 2022.

Këshilli i Lartë Gjyqësor, 'Përmbledhja e Diskutimeve: Regjistrimi Audio' <http://klgj.al/dokumentimi-i-mbledhjes-plenare/> aksesuar me 15 korrik 2022

Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2021' <http://klgj.al/wp-content/uploads/2022/04/RAPORT-VJETOR-2021.pdf> aksesuar më 15 korrik 2022

Këshilli i Lartë Gjyqësor, 'Raport mbi gjendjen e sistemit gjyqësor dhe veprimtarinë e këshillit të lartë gjyqësor për vitin 2020' <http://klgj.al/wp-content/uploads/2021/06/Raporti-Vjetor-KLGJ-2020.pdf> aksesuar më 15 korrik 2022

Këshilli i Lartë Gjyqësor, 'Relacion mbi Projekt-Aktin "Për Miratimin e Raportit Vlerësues dhe Propozimit të Grupit Ndërinstitucional të Punës mbi Riorganizimin e Rretheve Gjyqësore dhe Kompetencave Tokësore të Gjykatave" <http://klgj.al/wp-content/uploads/2022/06/relacion-harta-gjyqesore-F-1-Mbledhje-Plenare.pdf> aksesuar më 3 gusht 2022.

Këshilli i Lartë Gjyqësor, 'Vendim Nr 47, date 08.02.2022 Për Miratimin e 'Raportit Vjetor mbi Veprimtarinë e Komisionit Komisionit të Planifikimit Strategjik, Administrimit dhe Buxhetit për vitin 2021' <http://klgj.al/wp-content/uploads/2022/04/RAPORTI-VJETOR-MBI-VEPRIMTARINË-E-KOMISIONIT-TË-PLANIFIKIMIT-STRATEGJIK-ADMINISTRIMIT-DHE-BUXHETIT-PËR-VITIN-2021"-BASHKELIDHUR-VENDIMIT-Nr.47-datë-08.02.2022.pdf> aksesuar më 10 korrik 2022

Ligji 7895/1995, "Kodi Penal i Republikës së Shqipërisë" [1995] Fletore Zyrtare 2 ndryshyar së fundmi me ligjin 24/2021, "Shfuqizimi i togfjalëshit "pa marrë më parë lejen nga organi kompetent sipas dispozitave të vecanta´ në paragrafin e parë të nenit 262 të Kodit Penal të Republikës së Shqipërisë, si i papajtueshëm me nenet 17, pika 1 dhe 47 të Kushtetutës së Republikës së Shqipërisë" Fletore Zyrtare 87 (Kodi Penal i Shqipërisë)

Ligji 8136/1996, "Për Shkollën e Magjistraturës" [1996] Fletore Zyrtare 21 (shfuqëzuar)

Ligji 8417/1998, "Kushtetuta e Republikës së Shqipërisë" [1998] Fletore Zyrtare 28 ndryshuar së fundmi me Ligjin 16/2022 (Kushtetuta e Republikës së Shqipërisë)

Ligji 8577/2000, "Për organizimin dhe funksionimin e Gjykatës Kushtetuese të Republikës së Shqipërisë" [2000] FZ 4 ndryhuar me Ligjin 99/2016

Ligji 8678/2001, "Për organizimin dhe funksionimin e Ministrisë së Drejtësisë" [2001] Fletore Zyrtare 27 ndryshuar së fundmi me Ligjin 40/2017 [2017] Fletore Zyrtare 85

Ligji 8811/2001 "Për organizimin dhe funksionimin e Këshillit të Lartë të Drejtësisë" [2001] Fletore Zyrtare 9 i ndryshuar (shfuqizuar)

Ligji 9049/2003, "Për deklarimin dhe kontrollin e pasurive, të detyrimeve financiare të të zgjedhurve dhe të disa nëpunësve publikë" [2003] Fletore Zyrtare 31 ndryshuar me Ligjin 105/2018

Ligji 9367/2005, "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike" [2005] Fletore Zyrtare 31 ndryshuar me Ligjin 44/2014

Ligji 9877/2008 "Për organizimin e pushtetit gjyqësor në Republikën e Shqipërisë" [2008] (shfuqëzuar)

Ligji 49/2012, "Për organizimin dhe funksionimin e gjykatave administrative dhe gjykimin e mosmarrëveshjeve administrative" [2012] Fletore Zyrtare 49 (shfuqëzuar)

Ligji 122/2013, "Për disa shtesa dhe ndryshime në ligjin nr. 8116, datë 29.03.1996 "Kodi i Procedurës Civile i Republikës së Shqipërisë" [2013] Fletore Zyrtare 180 ndryshuar.

Ligji 177/2014, "Për disa shtesa dhe ndryshime në ligjin nr. 8588, datë 15.3.2000, "për organizimin dhe funksionimin e gjykatës së lartë të republikës së shqipërisë" [2014] Fletore Zyrtare 217 me të cilin u ndryshua Ligji 8588/2000, "Për organizimin dhe funksionimin e Gjykatës së Lartë të Republikës së Shqipërisë" [2000] FZ 7 (shfuqëzuar)

Ligji 84/2016 "Për rivlerësimin kalimtar të gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë", i ndryshuar

Ligji 96/2016, "Për Statusin e Gjyqtarëve dhe Prokurorëve në Republikën e Shqipërisë" [2016] Fletore Zyrtare 208 ndryshuar së fundmi me Ligjin 50/2021, "Për disa shtesa dhe ndryshime në ligjin nr. 96/2016 "Për statusin e gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë" [2021] Fletore Zyrtare 71

Ligji 98/2016, "Për organizimin e pushtetit gjyqësor në Republikën e Shqipërisë" [2016] Fletore Zyrtare 209 ndryshuar nga Ligji 46/2021

Ligji 115/2016, "Për Organet e Qeverisjes së Sistemit të Drejtësisë" [2016] Fletore Zyrtare 231 ndryshuar

Muižnieks Nils, 'Në vijim të vizitës në Shqipëri nga 23 deri 27 shtator 2013' (CommDH(2014)1) <https://rm.coe.int/raport-nga-nils-muiznieks-komisioneri-per-te-drejtat-e-njeriut-i-keshi/16806db6cb> aksesuar më 25 qershor 2022

OSCE, *Drejt drejtësisë: Analizë e proceseve civile në gjykatat e rretheve gjyqësore* (OSCE 2013)

Reporter.al, 'Ecuria e Vetingut' (3 gusht 2022) <https://reporter.al/vetingu/> aksesuar më 3 gusht 2022

Transparency International, '2021 Corruption Perceptions Index' <https://www.transparency.org/en/cpi/2021> accessed 2 June 2022

Transparency international, *Corruption Perceptions Index 2021* (Transparency International 2022) <https://images.transparencycdn.org/images/CPI2021_Report_EN-web.pdf> aksesuar më 15 qershor 2022

UNODC, 'Corruption in Albania: Bribery as Experienced by the Population' (2011) <http://www.instat.gov.al/media/3587/corruption_in_albania.pdf> accessed 2 June 2022

Vendim i KLD-së nr. 261/2, datë 14.04.2010 "Për sistemin e vlerësimit të gjyqtarëve

Vendimi e Këshillit të Ministrave 972/2020, 'Për organizimin, funksionimin e përcaktimin e kompetencave të Qendrës së Teknologjisë së Informacionit për Sistemin e Drejtësisë' [2012] FZ 213

Venice Commission, 'Judicial Appointments: Report adopted by the Venice Commission at its 70th Plenary Session' (16-17 March 2007, CDL-AD(2007)028) <https://www.venice.coe.int/webforms/documents/CDL-AD(2007)028.aspx> aksesuar më 01 korrik 2022

TENDENCAT NË RRITJE TË DISKRIMINIMIT DHE INTOLERANCËS NËPËRMJET ZHVILLIMIT TË TEKNOLOGJISË DHE ROLI I DREJTËSISË PENALE

M.SC. KRISTINA PUCI[1]

M.SC. ARDITA KURTI[2]

Abstrakt

Në erën digjitale, zhvillimet teknologjike për garantimin e shërbimeve ecin me ritme më të shpejta se sa hartimi i një legjislacioni shoqërues, ku fjala është për sfidën e përshtatjes së legjislacionit me kërkesat e sistemeve të ndryshme teknologjike. Vitet e fundit aksesi i pakufi i teknologjisë ka pamundësuar ushtrimin e kontrollit mbi mënyrën se si përdoren pajisjet teknologjike dhe aksesi në rrjet. Përdorimi i teknologjisë ka treguar në praktikë se mund të shkojë deri në atë shkallë sa të cenojë të drejtat e garantuara nga aktet më të larta ndërkombëtare apo të drejtat kushtetuese. Një interes të veçantë për studim përbën përdorimi i teknologjisë në përhapjen e formave të diskriminimit dhe intolerancës, sidomos nëpërmjet gjuhës së urrejtjes.

Ndaj ky artikull ka në fokus ndikimin e mjeteve teknologjike në përdorimin e tyre në cenimin e të drejtave themelore, si dhe evidentimin e mekanizmave parandalues për mbrojtjen nga diskriminimi. Rrjedhimisht, në këtë punim trajtohen aspektet historike të zhvillimit të teknologjisë në raport me të drejtat e njeriut dhe mbrojtja juridiko-penale që ofrohet për mbrojtjen e këtyre të

1 Juriste, Drejtoria e Përgjithshme e Kodifikimit dhe Harmonizimit të Legjislacionit. Ministria e Drejtësisë. E-mail: kristinapuci20@yahoo.com

2 Juriste, Drejtoria e Përgjithshme Rregullatore për Çështjet e Drejtësisë, Ministria e Drejtësisë. E-mail: kurtiardita@gmail.com

drejtave.Nëpërmjet këtij punimi bëhet një analizë e detajuar e formave të diskriminimit të cilat janë të dënueshme nga legjislacioni penal, si dhe të atyre fenomeneve të cilët janë të prekshëm në përditshmëri, por nuk gjejnë një trajtim juridiko-penal të plotë për parandalimin e këtyre fenomeneve, si dhe ndëshkimin e autorëve. Zhvillimi teknologjik ka bërë që fenomeni i diskriminimit, në të gjitha format e tij, të jetë mjaft prezent në shoqërinë tonë por në kuadrin e brendshëm ligjor nuk janë të parashikuara të gjitha format e tij duke, mos pasur kështu instrumentet e duhura për parandalimin e fenomenit dhe ndëshkueshmerinë e autorëve. Në këtë material, ofrohet edhe një analizë referuar përafrimit të legjislacionit shqiptar me aktet e Bashkimit Evropian dhe standardet ndërkombëtare.Duke marrë parasysh kompleksitetin e ndikimit të teknologjisë në rritjen e formave të diskriminimit, në përfundim artikulli parashtron disa rekomandime të posaçme me qëllim adresimin e problematikave nëpërmjet politikave penale.

Fjalë kyçe: Diskriminim dhe intolerancë, gjuha e urrejtjes, teknologji, parandalim, ndëshkim.

I. Mbrojtja juridike që ofrohet për mbrojtjen nga diskriminimi dhe gjuha e urrejtjes

E drejta penale përbën një fushë mjaft dinamike që kërkon studimin e vazhdueshëm të formave me anë të së cilave cenohen marrëdhëniet juridike që mbrojnë të drejtat dhe liritë themelore të individëve. Referuar problemeve të identifikuara nga praktika dhe raporteve të organizmave të ndryshëm ndërkombëtar, gjithnjë e më shumë, po vihet re se zhvillimi i mjeteve teknologjike dhe rrjeteve informatike ka një ndikim të ndjeshëm në shtimin e veprave penale dhe krijimin e formave të reja të veprimtarisë kriminale. Zhvillimi i teknologjisë në ditët e sotme ndodh me një shpejtësi relativisht të lartë, e si rrjedhim shoqëria, organet ligjzbatuese dhe legjislacioni janë në dinamizëm të vazhdueshëm për të kapur ritmin e teknologjisë.

Përdorimi i teknologjisë në masë të gjerë ka padyshim anët e veta pozitive në shpejtësinë dhe saktësinë e ofrimit të shërbimeve, uljen e kostove, lehtësimin e ndërveprimit ndërpersonal, apo parandalimin e kriminalitetit. Por, ajo çfarë vihet re është se përdorimi i teknologjisë në mënyrë të pakontrolluar nga organet shtetërore dhe pa një kuadër ligjor të detajuar, mund të çojë nga në rritjen e kriminalitetit për shkak të lehtësisë që krijohet në kryerjen e veprave penale.

Gama e veprave penale që mund të konsumohen nëpërmjet pajisjeve elektronike dhe sistemeve të informacionit është aq e lartë, sa tashmë vëmendja e studiuesve të së drejtës është kthyer nga gjetja e zgjidhjeve dhe mekanizmave në parandalimin e kryerjes së këtyre veprimtarive kriminale. Ndaj një nga çështjet që kërkon më tepër vëmendje në epokën e sotme është zhvillimi i teknologjisë dhe impakti që ka në orientimin e marrëdhënieve shoqërore, marrëdhënieve juridike dhe funksionimin e shtetit në tërësi.

Fillimi i përdorimit të rrjeteve të komunikimit ka ecur me ritme të shpejta duke filluar që nga periudha e komunikimit nëpërmjet e-mail e blogëve të vegjël. Ndërsa tashmë komunikimi dhe rrjetet elektronike janë shndërruar në një industri të tërë që bazon ekzistencën e vetë jo më në komunikimin ndërpersonal por në zhvillimin e ekonomisë së përgjithshme, si dhe ka një ndikim të jashtëzakonshëm në fusha të rëndësishme të jetës publike, sidomos nëpërmjet kompanive të lobimit.

Pavarësisht se një pjesë e madhe e popullsisë e konsideron teknologjinë vetëm si mjet logjistik në lehtësimin e veprimtarive të përditshme ndërpersonale, në ditët e sotme interneti shkon shumë më përtej se rrjetet sociale, duke përfshirë vjedhjen e të dhënave personale, dëmtimin e sistemeve të rëndësishme shtetërore, mashtrimin kompjuterik, qarkullimin e kriptomonedhave, trafikimin *online* si dhe *dark web*. Megjithatë, hulumtim të veçantë kërkon mënyra e përdorimit të rrjeteve elektronike në cenimin e të drejtave të njeriut. Nisur nga vështrimi i mënyrës se si funksionon shoqëria sot, në nivel global, është tepër shqetësues fakti se nëpërmjet teknologjisë mund të cenohen të drejta të cilat konsiderohen si të drejta themelore.

E nëse të drejtat themelore vihen në diskutim, pa pasur vetëdijen se jemi përpara paligjshmërisë, vëmendja që duhet të marrë kjo çështje është imediate. Kjo pasi nëpërmjet mjeteve teknologjike mund të vërehet se cenohet rëndomtë e drejta e integritetit fizik, integritetit mendor, integritetit profesional, e drejta për jetë private, e drejta për ushtrimin e lirisë fetare, e drejta për barazi dhe mosdiskriminim në lidhje me racën, etninë, ngjyrën, gjuhën, shtetësinë, bindjet politike ose filozofike, gjendjen ekonomike, arsimore ose shoqërore, gjininë, identitetin gjinor, orientimin seksual, vendbanimin, gjendjen shëndetësore, përkatësinë në një grup të veçantë apo për çdo shkak tjetër, sipas përcaktimeve në nivel kombëtar dhe ndërkombëtar. Pra nga njëra anë rrjetet e komunikimit na vijnë në ndihmë por nga ana tjetër mund të përdoren si mjet për të abuzuar me të drejtën e lirisë së shprehjes duke tejkaluar limitet morale dhe duke kaluar në gjuhë diskriminuese, intolerancë, gjuhë urrejtje apo nxitje për ekstremizëm.

Cenimi i të drejtave themelore nëpërmjet diskriminimit apo gjuhës së urrejtjes mund të jetë shpesh në një shkallë aq të lartë sa shihet e nevojshme ndërhyrja me instrumente ndëshkues nëpërmjet të drejtës penale. Por kjo çështje paraqitet mjaft komplekse për shkak të balancës që ligjvënësi duhet të ruajë midis garantimit të së drejtës së shprehjes, luftimit të diskriminimit dhe kontrollit të ekstremizmit fetar.

Konceptet e diskriminimit, intolerancës dhe gjuhës së urrejtjes janë koncepte të lidhura me njëra tjetrën. Diskriminimi në vetvete është dallim, veçim ose trajtim i padrejtë i një personi për të gëzuar lirisht apo për të përfituar nga ofrimi i shërbimeve publike a private, ndërsa intoleranca konsiderohet se është mungesa e respektit për praktikat ose besimet e tjera si dhe refuzimi i personave që janë të ndryshëm për shkak të etnisë, orientimit politik apo seksual. Intoleranca mund të shfaqet në një gamë të gjerë veprimesh duke filluar nga shmangia përmes gjuhës së urrejtjes deri te lëndimi fizik apo edhe vrasjet[3]. Krimet e motivuara nga intoleranca ose diskriminimi shpesh cilësohen edhe si krime urrejtjeje, mirëpo jo çdo formë diskriminimi konsiderohet si krim urrejtjeje. Në krimet e urrejtjes përfshihen vetëm ato vepra penale ku viktima është "zgjedhur" për shkak të një karakteristike të posaçme dhe nisur nga gjendja emocionale specifike dhe intensive[4]. Në shumicën e rasteve diskriminimi trajtohet nëpërmjet masave administrative apo nëpërmjet legjislacionit civil, por ajo që përbën interes për të drejtën penale janë rastet kur nëpërmjet diskriminimit, intolerancës apo gjuhës së urrejtjes cenimi i të drejtave është një shkallë të atillë që justifikon ndërmarrjen e masave ndëshkuese penale.

Ndërkohë lidhur me konceptin e gjuhës së urrejtjes nuk ka ndonjë përkufizim ligjor ndërkombëtar specifik, por është konsideruar si çdo lloj komunikimi në të folur, shkrim ose sjellje, që sulmon ose përdor gjuhë poshtëruese ose diskriminuese në lidhje me një person ose një grup të caktuar, në bazë të përkatësisë së tyre siç mund të jenë feja, përkatësia etnike, kombësia, raca, ngjyra, prejardhja, gjinia apo faktorë të tjerë identifikues. Këto elementë gjenerojnë intolerancë dhe urrejtje dhe në kontekste të caktuara mund të jenë nënçmuese, përçarëse dhe mund të sjellin edhe pasoja fatale. Kjo pasi nxitja nëpërmjet gjuhës së urrejtjes dhe intolerancës është një formë shumë e rrezikshme e të folurit, e cila në mënyrë eksplicite dhe

3 https://www.coe.int/en/web/compass/discrimination-and-intolerance#:~:text=Discrimination%20and%20intolerance%20are%20often,of%20perpetuated%20forms%20of%20prejudice. Aksesuar më datë 04.06.2022.

4 OSCE Office for Democratic Institutions and Human Rights (ODIHR), "Hate Crime Laws. A Practical Guide", 2009, fq 16-17.

të qëllimshme shkakton diskriminim, armiqësi dhe dhunë, të cilat mund të eskalojnë deri në akte terroriste apo mizore[5]. Referuar rekomandimit R(97) 20 të Komitetit të Ministrave[6], termi "gjuhë urrejtjeje" do të kuptohet se mbulon të gjitha format e shprehjes që përhapin, nxisin, promovojnë ose justifikojnë urrejtjen racore, ksenofobinë, antisemitizmin ose forma të tjera urrejtjeje të bazuara në intolerancë, duke përfshirë intolerancën e shprehur nga nacionalizmi dhe etnocentrizmi agresiv, diskriminimi dhe armiqësia ndaj minoriteteve, emigrantëve dhe njerëzve me origjinë emigrante.

Lidhur me mbrojtjen juridike që ofrohet në rastet e diskriminimit, intolerancës apo gjuhës së urrejtjes legjislacioni ndërkombëtar ka një "llojshmëri" mbi parashikimet ligjore lidhur me formën, mënyrën, ndëshkueshmërinë dhe mbrojtjen që i bëhet ndaj këtij fenomeni.

Për sa i përket instrumentave ndërkombëtare, Deklarata Universale e të Drejtave të Njeriut (DUDNJ), ndonëse ka karakter thjesht deklarativ dhe konsiderohet si një dokument "*soft law*", në nenin 7 parashikon se të gjithë janë të barabartë para ligjit dhe kanë të drejtë pa asnjë diskriminim të mbrohen barabartë nga ligji. Të gjithë kanë të drejtën për t'u mbrojtur në mënyrë të barabartë kundër çdo diskriminimi që cenon këtë Deklaratë, si dhe kundër çdo nxitje për një diskriminim të tillë.

Ndërkohë, Konventa Evropiane e të Drejtave të Njeriut si akti më i lartë në juridiksionin territorial të Këshillit të Evropës, në nenin 14 parashikon se gëzimi i të drejtave dhe i lirive të përcaktuara në këtë Konventë duhet të sigurohet, pa asnjë dallim të bazuar në shkaqe të tilla si seksi, raca, ngjyra, gjuha, feja, mendimet politike ose çdo mendim tjetër, origjina kombëtare ose shoqërore, përkatësia në një minoritet kombëtar, pasuria, lindja ose çdo status tjetër.

Një tjetër instrument normativ tepër i rëndësishëm lidhur me veprat penale të diskriminimit/gjuhës së urrejtjes të kryera nëpërmjet mjeteve teknologjike është Konventa Evropiane kundër krimit kibernetik (Konventa e Budapestit) dhe protokolli i saj shtesë në lidhje me kriminalizimin e akteve raciste dhe ksenofobike të kryera përmes sistemeve kompjuterike[7]. Protokolli kërkon që

5 Strategjia dhe Plani i Veprimit të Kombeve të Bashkuara kundër gjuhës së urrejtjes, 2019 https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf Aksesuar më datë 08.06.2022.

6 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680505d5b Rekomandimi i Komitetit të Ministrave. Aksesuar më datë 04.06.2022.

7 Protokolli shtesë i Konventës së Budapestit https://rm.coe.int/168008160f Aksesuar më datë 01.06.2022.

shtetet të miratojnë rregulla dhe masa të tjera që mund të jenë të nevojshme për të përcaktuar si vepër penale kryerjen me dashje dhe pa të drejtë të shpërndarjes ose vënies në dispozicion të tyre, të materialeve raciste dhe ksenofobike për publikun përmes sistemeve kompjuterike.

Protokolli parashikon se "material racist dhe ksenofobik" nënkupton çdo material të shkruar, çdo imazh, përfaqësimi i ideve ose teorive të cilat mbrojnë, promovojnë ose nxisin urrejtje, diskriminim ose dhunë, kundër një individi ose një grupi individësh, për shkaqe që lidhen me racën, ngjyrën, prejardhjen, origjinën, kombësinë, etninë, fenë, si dhe fenë nëse përdoret si pretekst për cilindo nga këta faktorë. Protokolli kërkon gjithashtu që shtetet të miratojnë masa ligjore për të ndëshkuar sjellje që konsistojnë në kërcënime apo fyerjeve publike, nëpërmjet një sistemi kompjuterik, të cilat kryhen me dashje dhe në mënyrë të padrejtë ndaj personave që i përkasin një grupi të caktuar, për shkaqe që lidhen me racën, ngjyrën, prejardhjen, origjinën, kombësinë, etninë, fenë, si dhe fenë nëse përdoret si pretekst për cilindo nga këta faktorë.

Rekomandimi R(97) 20 kundër gjuhës së urrejtjes i Komitetit të Ministrave u rekomandon shteteve anëtare që të marrin hapat e duhur për të luftuar gjuhën e urrejtjes dhe të sigurojnë një qasje gjithëpërfshirëse ndaj fenomenit, duke theksuar se shtetet duhet të krijojnë një kuadër ligjor të plotë të përbërë nga dispozita të ligjit civil, penal dhe administrativ mbi gjuhën e urrejtjes, të cilat u mundësojnë autoriteteve administrative dhe gjyqësore të garantojnë në çdo rast respektimin e lirisë së shprehjes dhe dinjitetin njerëzor.

Ndërsa, në Bashkimin Evropian mbrojtja ndaj veprave penale që kryhen për shkaqe raciste apo ksenofobike realizohet nëpërmjet vendimit kuadër të Bashkimit Evropian për luftimin e formave dhe shprehjeve të racizmit dhe ksenofobisë nëpërmjet ligjit penal (2008/913/JHA)[8] i cili parashikon detyrimin për shtetet anëtare të BE për të parashikuar dënime efektive, proporcionale dhe bindëse në rastin e kryerjes së krimeve raciste dhe ksenofobike.

Përveç rregullimit dhe parashikimit që bëjnë aktet ndërkombëtare lidhur me garantimin e të drejtave themelore dhe ndëshkimin e formave të diskriminimit, legjislacioni ynë i brendshëm parashikon një lloj "mbrojtje" të diskriminimit në përgjithësi. Legjislacioni shqiptar ka një sërë parashikimesh të cilat garantojnë mbrojtjen e të drejtave themelore si respektimi i gjinisë, etnisë, racës, fesë, orientimit seksual apo mbrojtjen e të drejtave të tjera, por

8 Vendimi Kuadër 2008/913/JHA i Bashkimit Evropian https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32008F0913&from=en Aksesuar më datë 01.06.2022.

pa u ndalur në të gjitha format e tij në mënyrë eksplicite, sidomos kur bëhet fjalë për diskriminimin nëpërmjet zhvillimit të teknologjisë. Kushtetuta e Republikës së Shqipërisë parashikon në nenin 18 të saj se "Askush nuk mund të diskriminohet padrejtësisht për shkaqe të tilla si gjinia, raca, feja, etnia, gjuha, bindjet politike, fetare a filozofike, gjendja ekonomike, arsimore, sociale ose përkatësia prindërore".

Ndërkohë që vetë kuptimi i diskriminimit jepet në ligjin nr. 10221, datë 4.2.2010 "Për mbrojtjen nga diskriminimi", i ndryshuar. Ky ligj synon respektimin e parimit të barazisë dhe mosdiskriminimit në lidhje me racën, etninë, ngjyrën, gjuhën, shtetësinë, bindjet politike, fetare ose filozofike, gjendjen ekonomike, arsimore ose shoqërore, gjininë, identitetin gjinor, orientimin seksual, karakteristikat e seksit, jetesën me HIV/AIDS, shtatzëninë, përkatësinë prindërore, përgjegjësinë prindërore, moshën, gjendjen familjare ose martesore, gjendjen civile, vendbanimin, gjendjen shëndetësore, predispozicionet gjenetike, pamjen e jashtme, aftësinë e kufizuar, përkatësinë në një grup të veçantë, ose me çdo shkak tjetër. Çdo person ose grup personash që pretendojnë se ndaj tyre është ushtruar diskriminim, mund të paraqesin kërkesëpadi përpara gjykatës kompetente sipas përcaktimeve të Kodit të Procedurës Civile për dëmshpërblim ose, sipas rastit, të kryejnë kallëzimin përpara organeve kompetente për ndjekje penale.

Por pavarësisht parashikimeve ligjore duket që në shoqërinë tonë jo vetëm që kjo mbrojtje nuk merret në konsideratë nga personat që kanë tendencën të diskriminojnë, në një nga format e parashikuara, por duket që ka një tendencë në rritje të shkeljes së këtij parashikimi pavarësisht koshiencës që ka gjithsecili. Në momentin që të drejtat themelore cenohen nga subjekte të tjerë, shtetet nëpërmjet legjislacionit të brendshëm duhet të gjejnë mekanizma parandalues, ndëshkues apo restaurues për rivendosjen e të drejtave të shkelura. Teknologjia është produkt i shoqërisë, vlerave të saj, prioriteteve dhe madje edhe pabarazive të saj, përfshirë edhe ato që lidhen me racizmin dhe intolerancën. Diskriminimi dhe gjuha e urrejtjes janë shndërruar tashmë në një problematikë sociale dhe situata aktuale duket akoma më shumë alarmante për shkak të përdorimit pakufi të teknologjisë, që është një faktor shtesë në impaktin shoqëror dhe në shkallën e përhapjes së tyre, si dhe pamundësisë për kontrollimin e përpiktë të mënyrës së përdorimit të teknologjisë dhe të përmbajtjes së materialeve që qarkullojnë.

II. Parashikimi i formave të diskriminimit dhe gjuhës së urrejtjes në legjislacionin penal

Ndërkohë që format e diskriminimit përbëjnë vepër penale kur përmbushin elementët e parashikuara në Kodin Penal. Në kuadër të mbrojtjes së të drejtave në një nivel sa më gjerë të mundshëm dhe në kuadër të parandalimit të formave të diskriminimit, në Kodin Penal parashikohet një kategori e caktuar veprash penale që ka në thelb mbrojtjen nga diskriminimi, me çfarëdo lloj baze qoftë ai. Lidhur me parandalimin dhe luftimin e formave të diskriminimit nëpërmjet legjislacionit penal, në vijim, legjislacioni është përditësuar lidhur me ndëshkimin e formave të reja të diskriminimit me qëllim ndërtimin e një ambienti të përbashkët miqësor mes grupimeve të ndryshme. Legjislacioni shqiptar ka një sërë parashikimesh të cilat garantojnë mbrojtjen e të drejtave themelore, parandalimin e diskriminimit por njëkohësisht edhe ndëshkimin e shkeljeve kundër barazisë mes subjekteve.Në Kodin Penal janë inkriminuar fenomene të tilla si shpërndarja e materialeve raciste apo ksenofobike (neni 119/a)[9], fyerja me qëllime raciste apo ksenofobike (119/b)[10] apo kanosja me motive racizmi dhe ksenofobie (neni 84/a)[11]. Ky grup veprash penale ka si qëllim parandalimin e cenimit të të drejtave të subjekteve që i përkasin një grupi apo pakice të caktuar me bazë racore, etnie, feje apo orientimi seksual. Shtimi i këtyre veprave penale në Kodin Penal ka ardhur në kuadër të ratifikimit të protokollit të Konventës kundër krimit kibernetik.

Këto vepra penale konsistojnë në ofrimin në publik ose shpërndarjen e qëllimshme, nëpërmjet sistemeve kompjuterike, të materialeve me përmbajtje raciste ose ksenofobike, fyerjen e qëllimshme publike, nëpërmjet sistemeve kompjuterike, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, kanosjen serioze për vrasje ose plagosje të rëndë, që i bëhet një personi, nëpërmjet sistemeve kompjuterike, për shkak përkatësie etnike, kombësie, race apo feje. Veprat penale të sipërcituara mund të zbatohen në rastin kur nëpërmjet sistemeve kompjuterike kryhet kanosje serioze, shpërndahen mesazhe, thirrje apo shkrime që kanë përmbajtje diskriminuese me bazë etnie, kombësie, race apo feje pasi objekti i këtyre

9 "*Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve me përmbajtje raciste ose ksenofobike përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet".*

10 *"Fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet".*

11 *"Kanosja serioze për vrasje ose plagosje të rëndë, që i bëhet një personi, nëpërmjet sistemeve kompjuterike, për shkak përkatësie etnike, kombësie, race apo feje, dënohet me gjobë ose me burgim deri në tre vjet".*

dy veprave penale është pikërisht mbrojtja e subjekteve nga shpërndarja e materialeve që cenojnë grupime që i përkasin një race, etnie apo kombësie të caktuar. Në krahasim me kuptimin që ligji i posaçëm për diskriminimin jep, është e dukshme se ana objektive e këtyre veprave penale është më e ngushtë pasi zbatohet vetëm për shkaqe diskriminuese që lidhen me racën, etninë dhe kombësinë, ndërkohë që format e diskriminimit nëpërmjet sistemeve kompjuterike janë shumë më tepër se kaq. Lidhur me ndëshkimin, masat e dënimit për këto vepra penale janë relativisht të larta dhe kjo bëhet në kuadër të parandalimit të përgjithshëm që ligji penal ka në shoqëri. Shpërndarja e materialeve raciste ose ksenofobike dhe fyerja me motive racizmi ose ksenofobie përfshihen në kategorinë e kundërvajtjeve penale dhe dënohen me gjobë ose me burgim deri në dy vjet, ndërsa kanosja me motive racizmi dhe ksenofobie ndëshkohet me gjobë ose me burgim deri në tre vjet.Ndërsa në mënyrë të përgjithshme ligjvënësi e ka parashikuar kryerjen e veprave penale të shtyra nga motive diskriminimi në nenin 50 të Kodit Penal. Në vitin 2007 është shtuar shkronja "j" e cila parashikonte se kryerja e veprës penale e shtyrë nga motive që kanë të bëjnë me gjininë, racën, fenë, kombësinë, gjuhën, bindjet politike, fetare ose sociale përbën rrethanë për rëndimin e dënimit. Ndërkohë, me ligjin nr. 144/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar", kjo shkronjë është ndryshuar duke parashikuar se dënimi që jepet nga gjykata rëndohet në rastet kur vepra është kryer e shtyrë nga motive që kanë të bëjnë me gjininë, racën, ngjyrën, etninë, gjuhën, identitetin gjinor, orientimin seksual, bindjet politike, fetare ose filozofike, gjendjen shëndetësore, predispozicione gjenetike ose aftësinë e kufizuar. Shtimi i shkaqeve që përbëjnë rrethanë rënduese ka ardhur pikërisht në kuadër të formave të reja të diskriminimit në shoqëri. Kjo dispozitë është e aplikueshme për të gjitha llojet e veprave penale, duke ndikuar në masën e dënimit që jep gjykata.

Ndërkohë, vepra penale të zbatueshme në parandalimin dhe luftimin e diskriminimit dhe gjuhës së urrejtjes janë nxitja e urrejtjes ose grindjeve (neni 265 i Kodit Penal) dhe thirrja për urrejtje nacionale (neni 266 i Kodit Penal).

Thirrja për urrejtje nacionale e parashikuar nga neni 266 konsiston në vënien në rrezik të paqes publike duke bërë thirrje për urrejtje kundër pjesëve të popullsisë, duke i fyer ose shpifur për to, duke kërkuar përdorimin e dhunës ose të veprimeve arbitrare. Pavarësisht se Kodi Penal nuk parashikon motivin dhe mënyrën se si kryhet kjo vepër, është një dispozitë që gjen zbatim edhe në rastin e urrejtjes nacionale nëpërmjet mjeteve të

komunikimit elektronik, si dhe në rastet kur nxitja e urrejtjes për shkaqe që lidhen me diskriminimin për shkak të kombësisë. Gjithashtu, pavarësisht se kjo vepër penale nuk kërkon pasoja për tu konsideruar si e tillë, në fakt rrezikshmëria që mbart është tepër e lartë sepse mund të vendosë në rrezik paqen dhe sigurinë publike. Në aplikimin e kësaj dispozite organi procedues duhet të analizojë përmbajtjen e thirrjeve dhe motivin e kryerjes së veprës penale, pasi në raste të veçanta mund të gjejë zbatim edhe fyerja me qëllime raciste apo ksenofobike (neni 119/b) e cila është figurë e posaçme e fyerjes së pjesëve të caktuara të popullsisë si dhe përcakton mjetin e posaçëm nëpërmjet të cilit kryhet kjo vepër penale, e konkretisht nëpërmjet sistemit kompjuterik.

Në kuadër të mbrojtjes së qytetarëve që i përkasin pakicave të caktuara për të ushtruar lirisht të drejtat e tyre, ligjvënësi ka inkriminuar nxitjen e urrejtjes dhe grindjeve për shkak të rrethanave si raca, etnia, feja dhe orientimi seksual në nenin 265 të Kodit Penal. Neni 265 i Kodit Penal parashikon se: "*Nxitja e urrejtjes dhe e grindjeve, për shkak të racës, etnisë, fesë ose orientimit seksual, si dhe përgatitja, përhapja ose ruajtja, me qëllim përhapjen e shkrimeve me përmbajtje të tilla, e kryer me çdo mjet ose formë, dënohet me burgim nga dy deri në dhjetë vjet*".

Ky nen ka pësuar ndryshime nëpërmjet ligjit nr. 144/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar", i cili parashikon se nxitja e urrejtjes dhe e grindjeve, për shkak të racës, etnisë, fesë ose orientimit seksual, si dhe përgatitja, përhapja ose ruajtja, me qëllim përhapjen e shkrimeve me përmbajtje të tilla, e kryer me çdo mjet ose formë, dënohet me burgim nga dy deri në dhjetë vjet. Në këtë mënyrë është shtuar nxitja e urrejtjeve dhe e grindjeve për shkak të orientimit seksual si dhe është zgjeruar ana objektive e veprës penale nisur nga zhvillimi i shoqërisë dhe mjeteve me anë të të cilave mund të kryhet kjo vepër penale, me qëllim ofrimin e një mbulimi sa më të gjerë për viktimat e diskriminimit.

Megjithatë, shkaku i nxitjes së urrejtjeve apo grindjeve është mjaft i kufizuar, duke u kufizuar vetëm në shkaqe që lidhen me racën, etninë, fenë dhe orientimin seksual, duke lënë jashtë fushës së zbatimit të kësaj dispozite një sërë formash të tjera të cilat nxisin urrejtje në masë. Parashikimi i kësaj vepre penale në legjislacionin penal është një domosdoshmëri pasi nxitja e urrejtjes është jo vetëm e dëmshme për bashkëjetesën shoqërore por pasojat mund të jenë të shumta dhe të rënda në varësi të intensitetit që kjo vepër kryhet dhe efekteve që prodhon tek personat që nxiten për të kryer akte që bien ndesh me rendin dhe paqen publike.

Ana objektive e veprës penale është nxitja e urrejtjes dhe e grindjeve si dhe përgatitja, përhapja ose ruajtja, me qëllim përhapjen e shkrimeve me përmbajtje diskriminuese, e cila është e përgjithshme, duke vendosur kornizat mbi ndëshkueshmërinë në rastin e nxitjes së urrejtjes me bazë diskriminimi apo përhapjen e shkrimeve të tilla. Ndërkohë që legjislacioni nuk përshkruan se çfarë do të konsiderohet nxitje apo deri në çfarë mase shkrimet do të konsiderohen të ligjshme dhe ku fillon paligjshmëria. Si rrjedhim mbetet në vlerësim të organeve proceduese për të vlerësuar rast pas rasti nëse ndodhemi para nxitjes së urrejtjes apo përhapjes së shkrimeve diskriminuese.

Ndërsa për sa i përket mënyrës dhe mjetit të kryerjes së veprës penale kjo vepër mund të kryhet në çdo mënyrë e cila i krijon autorit të veprës kushtet dhe mundësinë për të nxitur urrejtje apo përhapur shkrimeve që kanë përmbajtje diskriminuese. Në ditët e sotme këtë vepër penale mund ta ndeshim më tepër të kryer nëpërmjet mjetet e komunikimit publik për shkak të mundësisë që këto mjete ofrojnë për shpërndarjen e thirrjeve apo materialeve si dhe impaktin e shpejtë që kanë në përcjelljen e kontentit.

Nga ana procedurale veprat penale të sipërcituara mund të ndiqen penalisht edhe kryesisht, ndërsa vepra penale e fyerjes me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik, e parashikuar nga neni 119/b mund të procedohet vetëm nëpërmjet akuzës së ngritur nga viktima akuzuese[12]. Në rastin e fyerjes me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik barra e provës për të provuar ekzistencën e veprës penale bie mbi viktimën, gjë e cila mund të stepë viktimat për të filluar një proces penale kundër autorit apo autorëve pasi hetimi për të identifikuar autorët nëpërmjet sistemit kompjuterik është një proces jo i lehtë.

Por edhe për organin e prokurorisë hetimi i këtyre veprave penale nuk është mjaft komod për shkak se veprat penale kryhen në distancë e shpesh edhe në mënyrë të anonimizuar. Përveç kësaj, detyrë e prokurorisë është të vlerësojë ekzistencën e veprës penale duke shqyrtuar dhe vlerësuar nëse kemi të bëjmë më fyerje, diskriminim, gjuhë urrejtjeje apo fakti përfshihet në kuadrin e lirisë së shprehjes.

Ndërhyrja në ligjin penal për të parandaluar dhe luftuar diskriminimin dhe gjuhën e urrejtjes nuk është një proces i lehtë. Legjislatori duhet të ruajë balancën e duhur mes lirisë së shprehjes dhe ndëshkimin me efikasitet të diskriminimit dhe gjuhës së urrejtjes. Por pyetja që lind në këtë rast është se si mund ta dallojmë nëse një thirrje përmban gjuhë të urrejtjes apo thirrje

12 Kodi i Procedurës Penale të Republikës së Shqipërisë, neni 59, paragrafi 1.

diskriminuese?

Duke qenë se në Shqipëri nuk ka një praktikë të unifikuar mbi procedimin e këtyre veprave penale, vlen të shqyrtohet praktika e huaj dhe standardet ndërkombëtare për të qartësuar se kur kemi të bëjmë më një vepër penale që lidhen me diskriminimin, intolerancën, gjuhën e urrejtjes etj.

III. Standardet ndërkombëtare mbi ndëshkueshmërinë e formave të diskriminimit, intolerancës dhe gjuhës së urrejtjes dhe raporti me të drejtën për lirinë e shprehjes

Në kuadër të garantimit të së drejtës së individit për mbrojtje nga diskriminimi, intoleranca apo gjuha e urrejtjes duhet të merret në konsideratë e drejta e lirisë së shprehjes. Mendimi ndryshe nuk është gjithnjë diskriminim apo intolerancë, ndaj është detyrë e studiuesve të së drejtës dhe organeve përkatëse të lëvrojnë këtë fushë për të qartësuar ndarjen mes lirisë së shprehjes dhe fushëveprimit të së drejtës penale nëpërmjet ndëshkimit të veprimtarive që dalin përtej kësaj të drejte.

Liria e shprehjes gëzon mbrojtje nga Kushtetuta e Republikës së Shqipërisë (neni 22 dhe 23), si dhe aktet ndërkombëtare si Konventa Evropiane për të Drejtat Themelore të Njeriut (neni 10), Deklarata Universale e të Drejtave të Njeriut dhe Pakti Ndërkombëtar për të Drejtat Civile dhe Politike, si një nga të drejtat themelore të njeriut. Liria e shprehjes duhet t'i garantohet kujtdo pa asnjë lloji diskriminimi, me përjashtim të rasteve kur kjo e drejtë cenon një të drejtë tjetër themelore.

Lidhur me raportin që krijohet mes të drejtës së lirisë së shprehjes, referuar të drejtës evropiane e konkretisht, gjuha e urrejtjes e përdorur ndaj grupeve të caktuara fetare është në kundërshtim me vlerat që Konventa mbron, veçanërisht tolerancën, paqen dhe mosdiskriminimin. Rrjedhimisht kushdo që kryen akte të urrejtjes nuk mund të përfitojë nga mbrojtja që ofrohet nga neni 10 i Konventës mbi të drejtën për lirinë e shprehjes. Askush nuk lejohet të abuzojë me të drejtën e tij/saj për lirinë e shprehjes për të cenuar ose pakësuar padrejtësisht të drejtën për respektimin e të drejtave të të tjerëve (e sidomos të drejtën e besimit fetar)[13]. Të njëjtin qëndrim mban Komisioni Evropian kundër Racizmit dhe Intolerancës (ECRI) nëpërmjet

13 Venice Commission report "On the relationship between freedom of expression and freedom of religion: the issue of regulation and prosecution of blasphemy, religious insult and incitement to religious hatred, 2008, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2008)026-e Aksesuar më datë 16.06.2022.

Rekomandimit nr.7 të Politikës së Përgjithshme mbi legjislacionin kombëtar për të luftuar racizmin dhe diskriminimin racor. Në disa shoqëri demokratike sanksionimi në ligjin penal i formave të shprehjes që përhapin, nxisin, nxisin ose justifikojnë urrejtjen e bazuar në intolerancë është mëse i justifikueshëm, me kusht që çdo kufizim apo dënim i vendosur të jetë në proporcion me qëllimin legjitim të ndjekur[14].

Po kështu, referuar Planit të Veprimit të Rabatit të Këshillit të të Drejtave të Njeriut në OKB[15], është sugjeruar që diskriminimi apo gjuha e urrejtjes të përbëjnë vepër penale pasi të kalohet testi mbi**: kontekstin e gjuhës së përdorur**, **statusi i subjektit**, **qëllimi** (neglizhenca në gjuhën e përdorur nuk mund të konsiderohet si shkak i mjaftueshëm për konsumimin e veprës penale), **përmbajtja dhe forma, shtrirja e thirrjes** (natyra publike apo private, mjetet e shpërndarjes etj) **si dhe mundësia e reagimit nga audienca** (pavarësisht se vepra mund të quhet e kryer që në momentin e thirrjes, pa qene e nevojshme një pasojë, organet proceduese kanë detyrën të vlerësojnë mundësinë e reagimit nga subjektet pasive).

Rrjedhimisht, ndërhyrja në nivel kombëtar duhet të jetë e mirërregulluar në ligj, proporcionale dhe e diktuar nga nevoja për këtë ndërhyrje. Në të njëjtën logjikë është hartuar edhe Rezoluta 16.18 e Kombeve të Bashkuara "Për luftimin e intolerancës, stereotipave negative, stigmatizimit dhe diskriminimit, nxitjes së dhunës bazuar në fe ose besim", e miratuar në vitin 2011, e cila sugjeron për shtetet, ndër të tjera, që të miratojnë masa ligjore për të kriminalizuar nxitjen për dhunë bazuar në fe ose besim[16]. Edhe Pakti Ndërkombëtar për të Drejtat Civile dhe Politike në nenin 20 parashikon se çdo propagandë për luftime, mbrojtja e urrejtjes kombëtare, racore ose fetare që përbën nxitje për diskriminim, armiqësia ose dhuna duhet të ndalohen me ligj, mirëpo ligjvënësi duhet të ndërhyrë në nivel kombëtar për të garantuar rregullimin e marrëdhënieve juridike në mënyrën më të përshtatshme për të mos penguar ushtrimin e lirive dhe të drejtave themelore si dhe cenimin e të drejtave të të tjerëve.

Referuar jurisprudencës së Gjykatës Evropiane për të Drejtat e njeriut (GJEDNJ), në praktikën e saj, në çështjen *Delfi AS kundër Estonisë* (në vitin 2015) ku ka shqyrtuar për herë të parë përgjegjësinë e subjekteve për komentet e bëra në faqe *online* në internet, gjykata ka vendosur në dukje

14 Po aty._

15 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/101/48/PDF/G1310148.pdf?OpenElement Aksesuar më datë 13.06.2022.

16 https://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/a.hrc.res.16.18_en.pdf Aksesuar më datë 13.06.2022.

përfitimet nëpërmjet internetit dhe rreziqeve të tij lidhur me mundësinë e përhapjes së gjuhës së urrejtjes dhe nxitjes së dhunës. GJEDNJ ka vënë në dukje se natyra e komenteve mund të përbëjë nxitje urrejtjeje ose dhunë kundër një grupi të caktuar. Në rastet ku komentet e përdoruesve shfaqen në formën e gjuhës së urrejtjes dhe kërcënimeve të drejtpërdrejta ndaj integritetit fizik të individëve, Gjykata ka vlerësuar se të drejtat dhe interesat e të tjerëve dhe të shoqërisë në tërësi mund t'u japin të drejtë shteteve të vendosin masa ndëshkuese. Vlerësimi në çdo rast duhet të bëhet duke marrë parasysh natyrën ekstreme të komenteve dhe masa ndëshkuese të jetë proporcionale.[17] Po kështu, në çështjen *MTE dhe Index.hu Zrt kundër Hungarisë* (2016) GJEDNJ ka theksuar se portalet e lajmeve në internet kanë përgjegjësi dhe detyra lidhur me përmbajtjen e postimeve. Në çështjen konkrete Gjykata konstatoi se organet gjyqësore nuk kishin kryer vlerësimin e duhur mbi ruajtjen e balancës mes të drejtës për lirinë e shprehjes dhe të drejtës së faqeve të internetit të pasurive për të respektuar reputacionin e tyre tregtar, duke e gjetur Hungarinë në shkelje të nenit 10 (e drejta e lirisë së shprehjes) të Konventës. Edhe në çështjen *Angelova dhe Iliev kundër Bullgarisë* GJEDNJ i ka mëshuar parimit të propocionalitetit mes të drejtës së kufizuar dhe ndërhyrjes së ligjvënësit duke theksuar se krimet që janë veçanërisht të rënda, duke përfshirë ato që shkaktojnë dëme të shtuara për individët dhe shoqërinë, si krimet e urrejtjes, kërkojnë dënim proporcional sipas ligjit.

Në çështjen *Leroy kundër Francës* (2008) GJEDNJ ka theksuar se provokimi për një reagim të caktuar publik, i aftë për të nxitur dhunë dhe për të demonstruar një ndikim të besueshëm në rendin publik është në tejkalim të së drejtës për lirinë e shprehjes. Në këtë kuadër, heqja e materialeve nga *web*-i apo ndëshkimi i personit është një masë e justifikueshme. (Në rastin konkret kërkuesi ankohej për ndëshkimin e marrë për shkak të një publikimi ku mbështeste sulmin e bërë në 11 shtator 2001 ndaj Qendrës Botërore të Tregtisë[18].

Në Gjermani, për shembull, rregullat e miratuar së fundmi u kërkojnë kompanive të teknologjisë që të fshijnë përmbajtjet "qartësisht të paligjshme" brenda 24 orëve nga njoftimi. Përmbajtjet e tjera të paligjshme duhet të shqyrtohen brenda shtatë ditëve nga raportimi dhe më pas të fshihen. Nëse kërkesat e menaxhimit të ankesës nuk plotësohen, mund të shqiptohen gjoba

17 https://rm.coe.int/factsheet-on-hate-speech-july2018-docx/16808c168d fq 17. Aksesuar më datë 13.06.2022.

18 https://rm.coe.int/factsheet-on-hate-speech-july2018-docx/16808c168d fq 10. Aksesuar më datë 13.06.2022.

deri në 50 milionë euro[19].

IV. Impakti i teknologjisë në rritjen e diskriminimit dhe intolerancës dhe mekanizmat e përshtatshëm për luftimin e fenomenit

Platformat kompjuterike mund të përdoren, dhe janë përdorur tashmë, për të nxitur urrejtje kundër komuniteteve fetare ose për të mobilizuar reagime armiqësore ose të dhunshme ndaj shprehjeve fyese. Rrethanat që mund të jenë tregues të krimeve të intolerancës mund të përfshijnë motive si raca, feja, përkatësia etnike/kombëtare, statusi i aftësisë së kufizuar, gjinia ose orientimi seksual, përkatësia në një grup të caktuar, etj[20]. Liria e fesë dhe toleranca fetare janë vlera themelore të pranishme në çdo vend evropian, por aktet e diskriminimit hasen rëndomtë. Intoleranca fetare shpesh lidhet me racizmin dhe ksenofobinë, veçanërisht me antisemitizmin dhe islamofobinë.

Platformat *online* kanë revolucionarizuar komunikimin publik, duke i dhënë mundësi subjekteve të shprehin pikëpamjet e tyre, të cilat fatkeqësisht shpesh konsistojnë në diskriminim, armiqësi, dhunë ose fyerjen e komuniteteve fetare. Tanimë me rritjen e faqeve të mediave sociale me një nivel minimal censurimi dhe kontrolli të përmbajtjes së publikuar, e drejta e lirisë së shprehjes në internet është shfrytëzuar negativisht. Grupet kriminale dhe terroriste kanë demonstruar potencialin që platformat *online* të përdoren për të propaganduar ekstremizmin e dhunshëm fetar ose për të nxitur dhunën kundër pakicave fetare[21]. Jo vetëm në Shqipëri, por në rang global ligjvënësit janë duke u përballur me një sfidë të vështirë për t'iu përgjigjur fenomeneve që ndodhin në rrjetet e komunikimit të cilat nxisin personat të diskriminojnë apo të përjetësojnë akte armiqësore e të dhunshme në emër të fesë ose besimit.

Incidentet që përfshijnë gjuhën e urrejtjes, stereotipat negative dhe mbrojtjen e urrejtjes fetare ose kombëtare kanë rezultuar në vrasje, sulme në kultet fetare dhe thirrje për hakmarrje. Plani i Veprimit i OKB-së (Plani i Rabatit) thekson përgjegjësinë kolektive të zyrtarëve publikë, udhëheqësve fetarë dhe të komunitetit, mediave dhe individëve, si dhe nevojën për të

19 Po aty.

20 *Një shembull i përdorimit të teknologjive dixhitale në zhvillim, i motivuar nga paragjykimet, është përdorimi i Facebook-ut nga grupet radikale nacionaliste budiste dhe aktorët ushtarakë në Mianmar për të përkeqësuar diskriminimin dhe dhunën kundër myslimanëve dhe pakicave etnike. Në vitin 2018, shefi ekzekutiv i Facebook dëshmoi se sistemet e inteligjencës artificiale të Facebook nuk ishin në gjendje të zbulonin gjuhën e urrejtjes në kontekste të tilla.*

21 Raporti i Raportuesit Special të Kombeve të Bashkuara "Liria e fesë apo e besimit", fq 14, 2019.

ushqyer ndërgjegjen sociale, tolerancën, respektin reciprok dhe dialogun ndërkulturor për të parandaluar nxitjen e urrejtjes. Gjuha e urrejtjes dhe ksenofobisë në internet hasen më shpesh pas sulmeve terroriste. Meqenëse normat kundër urrejtjes luajnë një rol të rëndësishëm në ndalimin e shprehjes së paragjykimeve, të kuptuarit se si sulmet terroriste mund të ndikojnë në fuqinë e normës sociale është thelbësore për të kuptuar reagimet e shoqërisë ndaj këtyre sulmeve[22].

Promovimi i gjuhës së urrejtjes për shkaqe fetare dhe racore është identifikuar si pjesë e aktiviteteve terroriste. Mediat sociale apo hapësirat teknologjike janë përdorur për të promovuar gjuhën e urrejtjes dhe rekrutimin e personave për t'i shërbyer aktiviteteve të organizatave terroriste[23]. Në një çështje të trajtuar nga autoritetet shqiptare, një qytetar shqiptar gjatë studimeve të tij jashtë shtetit, pasi u kthye në Shqipëri organizoi një grup personash në jug të Shqipërisë të cilët nëpërmjet WebPages promovuan këndvështrime ekstreme lidhur me predikimin e luftës në vendet e lindjes së mesme, duke nxitur urrejtje dhe dhunë kundër besimeve të tjera dhe duke mbështetur organizata terroriste, si dhe predikim mbi idetë radikale. Personat u akuzuam ndër të tjera për shkelje të nenit 265 të Kodit Penal[24].

Rrjedhimisht, është e nevojshme të shtohet fokusi në luftimin e formave të racizmit, gjuhës së urrejtjes, ksenofobisë dhe intolerancës, të cilat nëpërmjet teknologjisë kanë gjetur hapësira të reja për të shpërndarë dhe për të nxitur thirrjet raciste dhe gjuhën e urrejtjes.

Për të përmbushur detyrimet e tyre për barazi dhe jo-diskriminim, autoritetet duhet të sigurojnë transparencë dhe llogaridhënie për përdorimin e teknologjisë digjitale në sektorin publik dhe të mundësojnë analiza dhe kontroll mbi këto sisteme. Në kuadër të zbatimit të politikave parandaluese, përveç inkrimiminimit të formave të diskriminimit dhe gjuhës së urrejtjes është e nevojshme të krijohen mekanizma apo autoritete për heqjen e përmbajtjeve me natyrë diskriminuese nga mjetet e komunikimit elektronik.

22 https://www.pnas.org/doi/10.1073/pnas.2007977117. Aksesuar më datë 20.06.2022.

23 *Referuar vëzhgimit të Raportuesit Special të OKB, emigrantët, refugjatët dhe personat pa shtetësi kanë raportuar se platformat e mediave sociale si Facebook, Twtter dhe Whatsapp përdoren shpesh për të përhapur urrejtje raciste dhe ksenofobike, dhe disa raportuan se janë shënjestruar drejtpërdrejt përmes mesazheve personale në këto platforma.* - Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement,2021.https://www.ohchr.org/en/documents/thematic-reports/ahrc4876-racial-and-xenophobic-discrimination-and-use-digital Aksesuar më datë 12.07.2022.

24 Studim krahasimor: "Forcimi i organeve të barazisë në rajonin e Ballkanit Perëndimor në fushën e gjuhës së urrejtjes, fq 9, 2020. https://rm.coe.int/raport-krahasimor-gjuha-e-urrejtjes-pdf/1680a0c258 Aksesuar më datë 12.07.2022.

Megjithatë, në respektim të standardeve ndërkombëtare mekanizmat parandalues duhet të jenë proporcional, pasi dhënia faktike e sanksioneve duhet gjithashtu të marrë në konsideratë rrezikun se ndëshkimet mund të sjellin ndërhyrje të papërshtatshme me lirinë e shprehjes[25].

Për t'ju përgjigjur situatës së krijuar shtetet (dhe kompanitë e teknologjisë) kanë miratuar masa që synojnë të luftojnë nxitjen kanë miratuar masa lidhur me raportimin për heqjen e menjëhershme të përmbajtjes që konsiderohet e paligjshme në rrjet[26]. Për shembull, për të luftuar përhapjen e gjuhës së paligjshme të urrejtjes në internet, në vitin 2016 është miratuar Kodi i sjelljes për luftimin e gjuhës së urrejtjes në internet, si masë administrative, i zbatueshëm nga kompanitë e mëdha (Facebook, Microsoft, Twitter dhe YouTube) për të ndihmuar përdoruesit që njoftojnë gjuhën e paligjshme të urrejtjes në këto platforma si dhe për të lehtësuar koordinimin me autoritetet kombëtare. Njoftimet duhet të vlerësohen brenda 24 orëve, duke respektuar gjithashtu legjislacionin e BE-së dhe atë kombëtar për gjuhën e urrejtjes, dhe hiqen nga platformat vetëm nëse vlerësohen si thirrje të paligjshme[27].

Ndërsa në Shqipëri ligji për mediat audiovizive rregullon fushën e transmetimit audioviziv duke garantuar që transmetimi të jetë në përputhje me të drejtën për informacion, e bindjeve politike dhe fetare, personalitetin, dhe dinjitetin si dhe me të tjera të drejta dhe liri themelore të njeriut, ndërkohë që komunikimi elektronik ende nuk gjen një rregullim të posaçëm për të shmangur diskriminimin, intolerancën dhe gjuhën e urrejtjes si dhe rregullimin e pasojave që shkaktohen nga këto veprimtari të paligjshme në sistemet kompjuterike. Ndryshimet në ligjin e medias, të cilat synojnë rregullimin e mediave *online* dhe disa aspekte të shpifjes, u miratuan nga Kuvendi në dhjetor të vitit 2019, por nuk u dekretuan nga Presidenti i Republikës, i cili e ktheu paketën në Kuvend për rishqyrtim me argumentimin se ndryshimet nuk janë në përputhje me standardet ndërkombëtare dhe parimet e lirisë së medias dhe ngrenë shqetësime në lidhje me rritjen e censurës dhe lirinë e shprehjes në vend.

Por në çdo rast, këto masa janë masa administrative të cilat merren nga autoritetet apo kompanitë pa pasur një proces penal për nxitje për urrejtje apo diskriminim, ndërkohë që sipas kuadrit të brendshëm ligjor mund të jetë e nevojshme që kjo masë të jepet edhe si masë plotësuese nga gjykata pas kryerjes së një procesi gjyqësor pasi është konstatuar ekzistenca e veprës

25 Rekomandimi nr. 15 i Politikës së Përgjithshme të ICRI për Luftimin e Gjuhës së Urrejtjes, 2016, fq 62.

26 Raporti i Raportuesit Special të Kombeve të Bashkuara "Liria e fesë apo e besimit", fq 14, 2019.

27 https://ec.europa.eu/newsroom/just/items/54300 Aksesuar më datë 20.06.2022.

penale.

Në rivendosjen e të drejtave të shkelura nga veprimtaritë e paligjshme, shtetet gjithashtu duhet të marrin masa për mbrojtjen e viktimave të veprave penale, duke shtuar fokusin ndaj tyre në rastet e diskriminimit, gjuhës së urrejtjes apo intolerancës. "Angazhimi dhe mbështetja e viktimave të gjuhës së urrejtjes" është një nga pikat e Planit të Veprimit të OKB. Shtetet duhet të solidarizohen me viktimat e gjuhës së urrejtjes dhe të zbatojnë masa të përqendruara në të drejtat e njeriut, të cilat synojnë të kundërshtojnë gjuhën hakmarrëse të urrejtjes dhe përshkallëzimin e dhunës. Shtetet gjithashtu duhet të nxisin masa për të siguruar që të drejtat e viktimave të respektohen dhe nevojat e tyre të adresohen, duke përfshirë mbrojtjen për mjete juridike, aksesin në drejtësi dhe këshillimin psikologjik .

Në Republikën e Shqipërisë aktualisht referuar ligjit për ndihmën juridike viktimat e diskriminimit kanë të drejtë të përfaqësohen me avokatë falas në çështjet gjyqësore që lidhen me rastet e diskriminimit. Megjithatë duhet parë mundësia për dhënien e ndihmës psikologjike pasi shpesh viktimat janë pre e bullizmit, urrejtjes dhe intolerancës, gjë që shkakton pasoja në cilësinë e jetës së tyre.

V. Konkluzione

Diskriminimi dhe gjuha e urrejtjes nëpërmjet mjeteve të komunikimit elektronik janë kthyer në forma të cenimit të të drejtave themelore. Krimet e motivuara nga intoleranca janë ndër shprehjet më të rënda të diskriminimit dhe përbëjnë një shkelje thelbësore të të drejtave themelore si dhe të nxisin krime nga më të rëndat si gjenocidi, krimet kundër njerëzimit, krimet e luftës apo veprat penale në fushën terroriste. Gjuha e urrejtjes është një kërcënim për vlerat demokratike, stabilitetin social dhe paqen dhe duhet të trajtohet në mënyrë që të parandalohen konfliktet e armatosura, krimet mizore dhe terrorizmi, dhe shkeljeve të tjera të rënda të të drejtave të njeriut.

Lidhur me diskutimin nëse gjuha e urrejtjes duhet të ndëshkohet me sanksione penale apo me masa administrative/civile, vlerësohet se gjuha e urrejtjes padyshim që justifikon vendosjen e sanksioneve penale. Në hartimin e legjislacionit duhet të bëhet përcaktimi i qartë i kritereve të anës objektive të veprave penale dhe masës së ndëshkimit, pasi është e rëndësishme që legjislacioni të jetë praktik, realist, i aplikueshëm dhe proporcional. Por që përmbajtja të konsiderohet si intolerancë apo gjuhë e urrejtjes duhet të vlerësohet konteksti i gjuhës së përdorur, statusi i subjektit, qëllimi,

përmbajtja dhe forma, shtrirja e thirrjes, si dhe mundësia e reagimit nga audienca._

Legjislatori shqiptar ka pasur si qëllim përafrimin me standardet ndërkombëtare në kuadër të mbrojtjes së çdo subjekti nga çdo lloji diskriminimi dhe përditësimi i legjislacionit është një objektiv i vazhdueshëm mbi ndëshkimin e formave të reja të diskriminimit me qëllim ndërtimin e një ambienti të përbashkët miqësor mes grupimeve të ndryshme. Mirëpo legjislacioni duhet riparë me qëllim përfshirjen e të gjithë formave të diskriminimit dhe rregullimin e pasojave, pasi përveç ndëshkimit të formave të diskriminimit dhe gjuhës së urrejtjes është e nevojshme të krijohen mekanizma për heqjen e përmbajtjeve me natyrë diskriminuese nga mjetet e komunikimit elektronik.

Problematikë përbën edhe zbatimi në praktikë i legjislacionit dhe mekanizmat e përshtatshëm për hetimin e këtyre veprave penale, për të ruajtur balancën mes të drejtës për lirinë e shprehjes dhe ndëshkimit të kriminalitetit.

Në praktikë haset problematikë edhe gjenerimi i të dhënave të sakta, pasi mbledhja e të dhënave për veprat penale të gjuhës së urrejtjes është e pamundur të realizohet, duke pasur në konsideratë edhe faktin se jo të gjitha shkeljet raportohen nga viktimat e diskriminimit.

Viktimave të diskriminimit dhe intolerancës duhet t'ju jepet mbështetje e posaçme psikologjike për tejkalimin e traumave të mundshme të shkaktuara nga stigmatizimi që u bëhen nëpërmjet mjeteve të komunikimit elektronik. Në këtë kuadër, duhet të forcohet roli i organeve shtetërore, shoqërisë civile dhe organizatave jofitimprurëse për mbështetjen e viktimave të gjuhës së urrejtjes si dhe rritjen e ndërgjegjësimit.

Lista e referencave

- Kushtetuta e Republikës së Shqipërisë;
- Konventa Evropiane e të Drejtave Themelore të Njeriut;
- Deklarata Universale e të Drejtave të Njeriut;
- Konventa e Këshillit të Evropës kundër krimit kibernetik,
- Protokolli shtesë i Konventës së Këshillit të Evropës kundër krimit kibernetik për kriminalizimin e akteve raciste dhe ksenofobike të

kryera përmes sistemeve kompjuterike;

- Kodi Penal i Republikës së Shqipërisë;
- Kodi i Procedurës Penale të Republikës së Shqipërisë;
- Ligji për mbrojtjen nga diskriminimi;
- Vendimi Kuadër i Bashkimit Evropian "Për luftimin e formave dhe shprehjeve të racizmit dhe ksenofobisë nëpërmjet ligjit penal" (2008/913/JHA);
- Rekomandimi i Komitetit të Ministrave R(97) 20 kundër gjuhës së urrejtjes;
- Rekomandimi nr. 15 i Politikës së Përgjithshme të ICRI për Luftimin e Gjuhës së Urrejtjes, 2016;
- OSCE Office for Democratic Institutions and Human Rights (ODIHR), "Hate Crime Laws. A Practical Guide", 2009;
- Strategjia dhe Plani i Veprimit të Kombeve të Bashkuara kundër gjuhës së urrejtes, 2019;
- Raporti i Raportuesit Special të Kombeve të Bashkuara "Liria e fesë apo e besimit", 2019;
- Raportuesi Special i OKB: Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement, 2021;
- Studim krahasimor: "Forcimi i organeve të barazisë në rajonin e Ballkanit Perëndimor në fushën e gjuhës së urrejtjes, 2020.
- Vendim i Gjykatës Evropiane për të Drejtat e Njeriut "Delfi AS kundër Estonisë" (2015);
- Vendim i Gjykatës Evropiane për të Drejtat e Njeriut "MTE dhe Index. hu Zrt kundër Hungarisë" (2016);
- Vendim i Gjykatës Evropiane për të Drejtat e Njeriut "Angelova dhe Iliev kundër Bullgarisë" (2007);
- Vendim i Gjykatës Evropiane për të Drejtat e Njeriut "Leroy kundër Francës" (2008);

https://www.coe.int/en/ëeb/compass/discrimination-and-intolerance#:~:text=Discrimination%20and%20intolerance%20are%20often,of%20perpetuated%20forms%20of%20prejudice

https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680505d5b

https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/101/48/PDF/G1310148.pdf?OpenElement

https://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/a.hrc.res.16.18_en.pdf

https://rm.coe.int/factsheet-on-hate-speech-july2018-docx/16808c168d

https://www.pnas.org/doi/10.1073/pnas.2007977117

https://ec.europa.eu/newsroom/just/items/54300

WHY BITCOIN MIGHT JUST BE THE BIGGEST PONZI SCHEME THAT EVER EXISTED?

BRUNILDA JANI HAXHIU
University of Tirana, Faculty of Law
brunajani@yahoo.com

Dr. ADRIAN LEKA
'Luigj Gurakuqi' University of Shkoder, Faculty of Law
leka-ad@live.com

Abstract

It is year 2022 and if you have not heard about Bitcoin, there's something wrong with you. The dream for immediate wealth has lived with humanity throughout history. In different periods, gold, bonds, even tulips, have had their turn to be considered secure investments from those wishing to earn as much in as little time. Now, it's cryptocurrencies. Bitcoin is the first fully digital currency in the world and one of about 80 cryptocurrencies have a market value of about 1 billion dollars.

There is hardly another economic or legal concept with such a diverse conceptualization around the world. Bitcoin's production, trade or possession in allowed or prohibited in different countries, and there are many other countries that have a more nuanced approach. Regulatory bodies are taking a very cautious approach towards it, but in different countries it is classified within different legal definitions: a currency, a commodity, but also an investment.

Similarly, researchers, investors, and the general public are divided in their views of Bitcoin. Some believe Bitcoin is the future of financial transactions and a secure investment. Other, in the opposite aisle, believe that it is nothing but a Ponzi scheme. This article will examine this second arguments and look into the legalities of Bitcoin in various jurisdiction, what creates the value in Bitcoin, how have value fluctuations impacted miners and investors. and what could happen in 2024 when the last Bitcoins would have been created. This analysis will lead to a conclusion on whether Bitcoin is, in fact, the new gold, or just something that is too good to be true.

Keywords: Bitcoin, Ponzi scheme, cryptocurrency, fraud, criminal law

Bitcoin – a brief history

Our modern economy depends to a large extent on traditional means of payment and, more and more lately, on digital means of payment. Traditional means of payment are based on bank transfers. Even in bank transfers, the money does not physically transfer from one bank to another, but still they require at least a few days to be confirmed. The underlying reason is that banks must prove to each other that the funds exist in the originating account, and that they are being transferred to the intended recipient. In these forms of payments, the problem of double spending is solved by requiring a series of verification steps, which on their side require a certain amount of time to be completed.

Modern commerce is mainly carried out in the form of e-commerce. E-commerce payment methods have a great need for the use of digital tokens. Electronic money is not a novelty for the economic literature. It has been present at least since the 1990s with the massive proliferation of electronic credit and debit cards or in the form of M-Pesa. In digital currency systems, the payment is simply a string of bits. The problem this poses is that bit strings, like any other digital record, may be copied and reused for another payment. So, digital tokens can be counterfeited and reused, which would cause a double spending issue. Presently, this is resolved by trusting a third party, which manages a centralized registry and transfers balances, through credits to sellers and debits to buyers. Often, this third party is the issuer of the digital currency itself and the value of the digital currency stems from the fact that scammers trust the third party to avoid double spending. The best example for this is PayPal.

The idea of cryptocurrencies[1] went a step further: towards removing the need for a third party. Cryptocurrencies are based on a decentralized network of validators (preferably anonymous) who maintain and update registry copies. This means that validators are at all times in consensus regarding the transaction records and each user's balance.

Although Bitcoin was the first fully consolidated cryptocurrency, there have been previous attempts to create online currencies with encrypted registers. Two examples of these are B-Money[2] and Bit Gold[3], which were formulated but not fully developed.

On October 31, 2008, a white paper was published on bitcoin.org[4] and distributed in a discussion forum on cryptography. The letter, written by Satoshi Nakamoto[5], explained a peer-to-peer electronic payment system, came to known as Bitcoin.

The Bitcoin infrastructure consists of an electronic transaction register and powerful computer units operated by private agents that are financially motivated by the operating protocol. The trust in this system is established by the blockchain technology, which ensures distributed verification, update and storage of transaction records. This is achieved through the creation of a blockchain. The block is a set of transactions that are conducted between Bitcoin users. The chain is created by a number of these blocks and contains the history of past transactions, which enables the creation of a public register, in which anyone can verify the amounts or units owned by each user. Therefore, the blockchain is like a book, containing the log of all the

1 Cryptocurrencies or virtual currencies are digital currencies issued by private individuals, which have no legal value guaranteed by a state or international institution. Their market value fluctuates as a result of individuals' demand for transactions or their expectations about the possible increase in the market price in the future. The electronic media uses a multitude of terminologies to refer to virtual currencies. In this paper, the terms "cryptocurrency", "digital currency" and "virtual currency" will be used as definitions with the same meaning, synonyms of each other.

2 B-Money was presented in 1998 by the computer scientist Wei Dai, but was never put into circulation. B-Money was designed as an anonymous and distributed payment system, and was very similar to modern cryptocurrency.

3 Bit Gold was one of the first efforts to create a decentralized virtual currency. It was introduced in 1998 by one of the blockchain pioneers, Nick Szabo. This project was never implemented, but it is believed that it inspired the Bitcoin protocol.

4 https://bitcoin.org/bitcoin.pdf

5 Satoshi Nakamoto is not a real person. His true identity has not been revealed until now, although there have been speculations about various persons, groups of persons and companies. Nakamoto's involvement with Bitcoin ended in 2010, when he sent an email stating that he "was moving into other things." It is believed that Nakamoto owns about 1 million Bitcoin. Satoshi is also the name of Bitcoin's smallest unit.

transactions that have been performed, while the blockchain is a new page that records all the current transactions.

The registry is decentralized. The private agents who maintain the system record the transactions in the only public copy of the register, thus leaving traces only in this unique register and not in each of their private registers. The reliability of the unique distributed register is guaranteed by the implementation of two schemes within the electronic protocol:

- Cryptographic elements to ensure security.
- Financial rewards that motivate agents to maintain the (decentralized) system infrastructure.

The financial reward of agents is especially important because the production of Bitcoin and the validation of transactions is costly[6]. The reward scheme is two-fold:

- Commission for carrying out and validating transactions.
- Subsidies enabled by the electronic protocol for the creation of new currencies (seniority).

The creation of new Bitcoin coins is accomplished by allowing brokers to compete for the right to update the chain with a new block. This competition happens as process known as "mining." Miners, which are actually transaction validators, compete to solve difficult mathematical problems, called *'proof-of-work'* (POW). The winner in the mining process has the right to update the chain with a new block, that is to create a new coin.

The registry cannot be manipulated without the consensus of the agents who maintain the system infrastructure. The consensus protocol stipulates that the *'longest'* history will be accepted as the confirmed public record (register). Cryptographic security and the decentralization of infrastructure make redundant the presence of an authority that guarantees the reliability of the system.

Blockchain based on the PoW consensus protocol handles transaction history by going backwards. This means that if someone tries to revoke a past transaction, they should propose another blockchain that does not

6 Bitcoin miners must use expensive hardware, if they want to have fast results. The hardware uses a large amount of electricity. Currently, the hardware spends about 176 USD of electricity per each Bitcoin transaction, while the mining of one Bitcoin uses between 7,000-11,000 USD of electricity. The cost of an ASIC machine related to the mining of one Bitcoin is between 15,000-19,000 USD. Given that the Bitcoin price on July 15, 2022 is about 20,000 USD, the costs associated with it are considerable.

contain that transaction, and perform a POW for each new proposed block. This means that it is very costly to rewrite the transaction history, which is an extra protection against double spending. Blockchain does not automatically protect against an attack that looks forward, although this does not seem very likely as well, due to the high costs that are associated with this work as well.

One of the Bitcoin's peculiarities is that its quantity is limited. The system is built in such a way that only 21 million Bitcoin can be produced. About 18 million have been produced so far[7] and it is estimated that production will be completed in 2024.

In 2009, the Bitcoin software was first released and, eventually, the Bitcoin production process began[8]. Until 2010, Bitcoin had not been traded, therefore it was not possible to assign a monetary value to it. In 2010, a person decided to use Bitcoin for the first time, exchanging 10,000 Bitcoin for two pizzas[9].

As Bitcoin grew in popularity, in 2011 the first alternative cryptocurrencies appeared. Among the first were Namecoin and Litecoin. In 2014, Bitcoin fell prey to a fraudulent scheme. The world's largest Bitcoin exchange platform, Mt.Gox, went offline and 850,000 Bitcoin disappeared. Their owners have not yet learned where these coins went. That same year, the Ethereum platform appeared, which uses the Ether cryptocurrency to enable smart contracts and blockchain-based applications. At the same time, several platforms emerged, in which investors could exchange their shares in the same way as cryptocurrencies are exchanged. These were immediately flagged as opportunities for fraud or pyramid schemes.

In November 2021, Bitcoin reached the highest recorded price, of 68,000 USD. Meanwhile many other coins have ended up following a scheme called *'rug pull.'* This means that when a certain popularity and price is reached,

7 The maximum Bitcoin quantity, as established in the blockchain, is 21 million. The real final number will be smaller, because it is believed that 2-3 million Bitcoin have been lost (the private access key has been lost, they have been sent to the wrong addresses, etc.)

8 On January 12, 2009, the first Bitcoin transaction occurred. Satoshi Nakamoto sent ten Bitcoin to Hal Finney, a renown cryptographer.

9 On May 22, 2010, Laszlo Hanyecz, a resident of Florida, exchanged his Bitcoin with two pizzas in a local Papa John's restaurant. This is recorded as the first Bitcoin usage for a purchase. In fact, it was not yet possible to use Bitcoin in commercial establishments, but Hanyecz wrote in Bitcointalk community forum that he would pass his Bitcoin on to the person that would buy him two pizzas. Given the Bitcoin value, these could be considered the most expensive pizzas of all time. Hanyecz was also one of the first Bitcoin coders and developers; he was the person that created the Bitcoin code for Mac OS.

the creators and their friends sell all the coins they have. Immediately, the price of the currency falls and the trade ends. The Coinopsy site lists several thousand *'dead'* coins.

Since November 2021, Bitcoin has also suffered reduced price and capital value. This was initially caused by the new bans that China imposed on its financial system[10]. Many new currencies have fallen by 90%.

What is Bitcoin from a legal perspective?

Bitcoin, similarly to other economic concepts, is not classified in the same way in all countries of the world. But there are hardly any other economic concepts that have such a different classification from one country to another. There are countries that allow Bitcoin to be produced, held, used, traded; there are countries that allow production, but not usage or trade; and there are countries that allow neither production nor trade. Most countries have restrictions that are more nuanced than the rigid categories above. Prohibitions and restrictions on Bitcoin come not only from economic considerations (protection of individuals, investors from investments, whose nature is still unclear), but also from other no less important considerations:

- The high energy consumption and its impact on the environment.
- Illegal production, which more often than not is driven by the desire to cut on electricity costs rather than from bans on production.
- Problems arising from the relative anonymity of Bitcoin holders.
- Jurisdictional problems that may arise and may make it difficult to investigate potential criminal activity.
- The possibility of using Bitcoin for money laundering and terrorist financing.

The general trend of national institutions has been a cautious public attitude and non-enthusiastic reactions to the developments in the virtual currency market. Their reserved attitude is part of the efforts to not encourage

10 In September 2021, China banned all cryptocurrency transactions. The official basis for this move was the effort to curtail financial crime and prevent economic instability. However, it has been argued that China's cryptocurrency ban came amid fears that cryptocurrencies were facilitating capital flight from its markets and, therefore, this ban was part of a new trend in Chinese economic policy toward greater state intervention. Despite the ground, this ban had huge effect on the global Bitcoin market.

or orient individuals' savings and monetary balances towards investing in virtual currencies. There is a consensus among monetary and international authorities that the technological innovation of Bitcoin's infrastructure poses the potential for at least two new opportunities. The first option is to expand the existing monetary policy framework through the issuance of a national digital currency, based on a technology similar to the Bitcoin's one. The second possibility is the implementation of blockchain technology in a version adapted to the operation and improvement of the current payment system.

At one extreme of these countries is China, where there have been persistent restrictions on Bitcoin until September 21, 2021, when a complete ban on all activity related to Bitcoin was imposed. At the other extreme stands, for example, Belarus, where President Lukashenko has urged citizens not to emigrate, but to stay there and produce Bitcoin.

Bitcoin has been called many other things over the years: digital money, digital gold, investment, commodity or even fraud, and the end of modern capitalism as we know it. Legally, Bitcoin is labeled as a currency, commodity or investment.

Bitcoin and gold – the differences

The most frequent comparison that is made to Bitcoin is to gold. This is mainly based on an emphasis of the fact that Bitcoin's value comes from its limited quantity and high demand in the market. However, this comparison is not perfect.

Gold today is mainly used as value storage, and no one pays in gold. Gold is also very static, while Bitcoin has not been that static so far. On the other hand, the amount of Bitcoin is really limited. Even Satoshi Nakamoto himself, if wanted to, could not change the maximum number of Bitcoins. As for gold, it is indeed in limited quantity, but not so decisively. Moreover, the universe is infinite and there is a possibility, at least theoretically, that gold will be discovered outside our planet.

Gold and Bitcoin differ in terms of history; gold has been in circulation since 700 BC, and Bitcoin since 2009. The market capitalization value of Bitcoin is approximately 800 billion dollars, while that of gold is 9 trillion dollars. They also differ in terms of transportability, which becomes important in times of crisis. The standard gold bar held by banks weighs 12.4 kg. Bitcoin weighs nothing because it is digital.

Thus, the comparison between Bitcoin and gold is not ideal, not only because of their physical qualities, but mainly because their duration in the market is very different and many years must pass in order for us to ascertain whether Bitcoin will behave like gold in the long-term perspective.

Bitcoin as a currency

Bitcoin can be used to buy a variety of things. From vacations, artwork, food, cars, real estate, etc. More than 100,000 different websites accept Bitcoin as a payment method. But for a currency to have a chance of success, it must have low volatility. If a currency fluctuates too much, it makes it difficult to properly assess the value of goods and services and, therefore, to manage the flow of income.

Most major currencies have an annualized volatility rate between 0.5% and 1% every 30-60 days. In 2018, Bitcoin hovered between 4-5%, but has been in decline ever since. Currently, volatility is down to 2.25%. But it is still far from the US dollar in terms of stability. So, while you can absolutely use Bitcoin to buy and sell things, it seems that it's seen as more valuable as something other than a currency.

Bitcoin as an investment

What if we look at Bitcoin as an investment, that is, as something we buy and hold, hoping the price will go up? In this respect there are two groups: those who support Bitcoin as an investment and those who oppose it.

On the side of Bitcoin supporters are companies like MicroStrategy and Square, which have made big bets on Bitcoin as an investment. Their take on Bitcoin's potential as an asset is two-fold. The first concerns its position as a money supply that is beyond the quantitative definitions currently used by some of the world's largest economies. No one and nothing can change the amount of Bitcoin. Its money supply is fixed and non-inflationary. The second lies in its ability to be an open platform for entire countries and territories that are currently not reached by financial services. Currently, 2.5 billion people do not use banks or microfinance institutions to save or borrow. Part of this depends on the banks' view of the benefits from these people versus the costs of going to them. But it also depends on the state of the currencies that many of the unbanked countries have to use.

But not everyone sees it that way. Others consider Bitcoin to be a poor

investment vehicle precisely because it does not conform to the structures and institutions of traditional money. They argue that, because there is no trusted institutional market for trading cryptocurrencies, this seems like an investment far beyond what economists would traditionally choose. The main reason is that Bitcoin is a zero-yield asset, so holding the asset does not produce any profit. The only profit that comes from Bitcoin is if it is sold at a higher price than it was bought for.

Bitcoin as a commodity

Commodities are basic goods that are interchangeable with other goods of the same type. Examples of commodities in the real world are: gold, oil, natural gas, etc. In recent years, more financial products have been added to the list of goods, one of which is Bitcoin. In America, the Commodity Futures Trading Commission defined Bitcoin as a commodity as early as 2015.

Commodities have traditionally had higher price volatility than assets, such as property, or money supplies, such as currencies, making them a favorable environment for speculators trying to predict the rise and fall of an asset accordingly. This is, in a way, futures trading, a market where people try to predict which way a commodity will swing.

Bitcoin as a commodity seems to work in two different investment directions: short-term, i.e., daily volatility, and long-term speculation. Additionally, Bitcoin as a commodity is more regulated than as a currency or investment. Because futures markets allow investors to speculate without having to hold the underlying asset, this has led to institutional interest in Bitcoin that has helped it be seen more as a commodity than anything else.

Bitcoin's advantages

The most distinctive features and advantages of Bitcoin are laid out below.

- It is decentralized - No one controls or owns the Bitcoin network and it has no leader. Of the thousands of cryptocurrencies in existence, Bitcoin is arguably the most decentralized, an attribute considered to strengthen its position as collateral for the global economy.
- It is distributed - All Bitcoin transactions are recorded in a public

ledger. The network relies on people voluntarily maintaining copies of the ledger and running the Bitcoin protocol software. These *'nodes'* contribute to the correct propagation of transactions across the network, following protocol rules defined by the software client. There are currently more than 80,000 nodes distributed globally, making it nearly impossible for the network to suffer interruptions or data loss.

- It is transparent - The addition of new transactions to the block book and the state of the Bitcoin network at any given time (in other words, the truth about who owns how many Bitcoins) is achieved by consensus and transparently according to the rules of the protocol.
- It is a peer-to-peer system - Although nodes store and propagate the state of the network (the *'truth'*), payments effectively go directly from one person or business to another. This means that there is no need for any trusted third party to act as an intermediary.
- There is no need for permission - Anyone can use Bitcoin, there are no authorizers and it is not necessary to create a Bitcoin account. All transactions that follow the rules of the protocol will be confirmed by the network based on the established consensus mechanisms.
- It is pseudo-anonymous - Identity information is not intrinsically linked to Bitcoin transactions. Instead, transactions are linked to addresses that take the form of randomly generated alphanumeric strings.
- It cannot be censored - Since all Bitcoin transactions that follow the rules of the protocol are valid, transactions are pseudo-anonymous, and users themselves own the key to their Bitcoin holdings, it is difficult for authorities to stop individuals from using it that or seize their Bitcoins. This carries important implications for economic freedom and may even act as a powerful force against authoritarianism globally.
- It is public - All Bitcoin transactions are recorded and publicly available for anyone to see. This virtually eliminates the possibility of fraudulent transactions, but also makes it possible, in some cases, to link individual identities to specific Bitcoin addresses. A number of efforts to improve Bitcoin's privacy are underway, but their integration into the protocol is ultimately subject to Bitcoin's quasi-political governance process.
- There is a fixed supply - One of the main parameters in the Bitcoin protocol is that the supply will expand over time to a final number of 21 million coins. This fixed and known total supply is argued to

make Bitcoin a *'hard asset',* one of several characteristics that has contributed to its perceived value from an investment perspective.

- The existence of disinflation - The rate at which new Bitcoins are added to the circulating supply gradually decreases along a defined schedule that is built into the code. Starting at 50 bitcoins per block (a new block is added approximately every 10 minutes), the issuance rate is halved approximately every four years. In May 2020, the third halving reduced the issuance rate from 12.5 to 6.25 bitcoins per block. At that point 18,375,000 of the 21 million coins (87.5% of the total) had been produced. The fourth halving, in 2024, will reduce the issuance to 3.125 BTC, and so on until approximately 2136, when the final halving will reduce the block reward to just 0.00000168 BTC.
- It is profit-driven - A core group of participants, known as producers, are driven by profit to contribute the resources needed to maintain and secure the network. Through the PoW process, they compete to add new blocks to the chain that makes up the blockchain. Hardware and energy costs contribute to network security in a decentralized manner according to principles driven by game theory. The profit motive is considered important in this respect. Further, since miners tend to sell their earned Bitcoin to cover costs, the mining process is seen as a fair mechanism for the wide distribution of bitcoins.

Why Bitcoin might just be a Ponzi scheme?

There are many voices in the economic and technological fields that affirm this. Brazilian computer scientist Jorge Stolfi was among the first. His view is based on the following observations:

- Investors buy in anticipation of profits.
- This expectation is supported by the profits of those who sell.
- There is no external source for the above profits, they come entirely from new investments.
- The operators themselves benefit a large part of the money.

On the first point, it is worth assessing how Bitcoin compares to the original pyramid scheme created by Charles Ponzi. In 1920, Ponzi promised 50% profit for a 45-day investment and managed to pay this profit to a number of investors. It managed to survive the departure and change of investors, until the scheme finally collapsed after less than a year.

In the largest and possibly longest running pyramid scheme in history, Bernie Madoff paid out about 1% profit per month. He offered the participants to return in cash both the original amount invested and the profit. The great financial crisis of 2008 led to the collapse of the scheme.

But the unraveling of Madoff's scheme has continued even after its collapse due to extraordinary and ongoing legal proceedings. These have continued even after Madoff's death in early 2021. One of the bankruptcy trustees, Irving H. Picard, persistently and successfully went after people who took more money out of the scheme than they put in. He even managed to trace the money to offshore accounts, taking the case all the way to the Supreme Court. Of the $20 billion in original known investments in the scheme (which victims were told had reached a value of more than three times that amount), about $14 billion (70%) has been recovered and distributed.

Unlike Madoff's investments, Bitcoin is purchased not as an income-earning asset, but as a perpetual coupon with zero value. In other words, it does not promise anything in the way of continued earnings and never matures so that the maturity value can be returned and claimed. In this sense, the only way to earn is to sell to another person.

The collapse of Bitcoin would look very different from that of a Ponzi or Madoff scheme. In such a case, it would not be possible to make any long-term legal effort to pursue those who have sold their Bitcoins in order to redistribute their profits to those left with Bitcoins. Bitcoin holders would have no claim against those who previously bought and sold.

In terms of cash flow, Bitcoin is more like a scheme known as pump-and-dump. In such a scheme, traders buy shares that have no value, advertise them and sell them to each other at inflated prices. When outsiders approach to buy them, they sell them and the scheme collapses. Similarly, Bitcoin taps into the pure desire for capital gains. Buyers can't stand others getting rich overnight.

Another big difference between Bitcoin and a Ponzi scheme is that the former is, from a social point of view, a game of many negatives. Because real resources are used to create and keep Bitcoin functioning, it is costly in a way that was not true of Madoff's two- or three-person operation. From a social point of view, what Madoff got out of his scheme was a zero-sum redistribution (they eventually sold their properties to pay for the losses), and Bitcoin's fall will be much worse than that, due to the investment beginner at it.

To conclude, the analysis of Bitcoin must recognize its uniqueness. As an object of speculation, Bitcoin is unprecedented on a large scale. It didn't start as a joke, but as a trillion-dollar asset. Unlike a pyramid scheme, Bitcoin cannot end with the escape of the one who started it.

References

Aitken, Roger (2016), "Danish Blockchain Startup Coinify Scores $4 Million Early-Stage Investment", Forbes, 03.08.2016, available at: http://www.forbes.com/sites/rogeraitken/2016/08/03/sebs-vc-unit-invests-4m-in-blockchain-payments-operator-with-seed-capital/#33e495b01ea1, accessed on May 13, 2022.

Berta, Michael A. and Noonan, Willow W. (2015), "The property-contract duality of Bitcoin", Financeworldwide, available at: https://www.financierworldwide.com/the-property-contract-duality-of-bitcoin/#.WFb1ZnSg_IU, accessed on May 17, 2022.

Boehm, Franziska and Pesch, Paulina (2014), "Bitcoin: A First Legal Analysis - with reference to German and US- American law", University of Munster.

Brito, Jerry et al. (2014), "Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, And Gambling", New York Law School.

Brito, Jerry (2015), "The Law of Bitcoin", iUniversity, Bloomington, U.S.A.

Cavadini, Federica (2014), "Dalla bistecca a palestra e taxi qui sipaga con moneta virtual", Corrieredella sera, 02.02.2014, available at: http://milano.corriere.it/milano/notizie/cronaca/14_febbraio_02/dalla-bistecca-palestra-taxi-qui-si-paga-moneta-virtuale-f1ab0942-8bf1-11e3-a29b-8636964bc663.shtml, accessed on April 14, 2022.

Changes in modus operandi of Islamic State terrorist attacks, Europol report, 18.01.2016, available at: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks, accessed on May 1, 2022.

Chavez-Dreyfuss, Gertrude (2014), "Exclusive: Overstock CEO says bitcoin sales to add 4 cents to 2014 EPS", Reuters, 13.08.2014, available at: http://www.reuters.com/article/us-overstock-com-bitcoin-idUSKBN0GD21220140813, accessed on April 13, 2022.

Chen, Adrian (2016), "We Need to Know Who Satoshi Nakamoto Is", the New Yorker, 09.05.2016, available at: http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is, accessed on May 4, 2022.

Castellano, Giuliano G. (2012), "Towards a General Framework for a Common Definition of "Securities": Financial Markets Regulation in Multilingual Contexts", Uniform Law Review.

European Central Bank, What is money?, 24.11.2015, available at: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html, accessed on June 13, 2022.

Grossman, S.J. and Hart, O.D., (1994), "The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration", Journal of Political Economy 94.

Guarascio, Francesco (2015), "EU clamps down on bitcoin, anonymous payments to curb terrorism funding", Reuters, 19.11.2015, available at: http://www.reuters.com/article/us-france-shoooting-eu-terrorism-funding-idUSKCN0T81BW20151119, accessed on May 15, 2022.

Hackett, Robert (2015), "New York Stock Exchange Gives Bitcoin Some Mainstream Love", Time, 19.05.2015, available at: http://time.com/3889775/new-york-stock-exchange-gives-bitcoin-some-mainstream-love/, accessed on May13, 2022.

Harrison, Virginia (2015), "This could be the first country to go cashless", CNN, 02.06.2015, available at: http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/, accessed on Jun 2, 2022.

Higgins, Stan (2016), "US Bankruptcy Court Set to Weigh in on Bitcoin's Currency Status", CoinDesk, 09.02.2016, available at: http://www.coindesk.com/bankrupt-bitcoin-mining-firm-trustee-seeks-return-of-funds-from-former-promoter/, accessed on May 22, 2022.

Kaplanov, Nikolei M. (2012), "Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulations", 25 Loy . Consumer Law Review # 111, 2012.

Malloy, Robin Paul and Diamond, Michael (2011), "The Public nature of Private property", Ashgate Publishing, U .S.A., 28.08.2012.

Maras, Elliot (2016), "A First In Denmark: Miner Buys House With Bitcoin Using Coinify", Cryptocoinsnews, 14.03.2016, available at: https://www.cryptocoinsnews.com/a-first-in-denmark-miner-buys-house-with-

bitcoin-using-coinify/, accessed on June 13, 2022.

Mattei, Ugo (2000), "Basic Principles of Property Law: A Comparative Legal and Economic Introduction", Greenwood Publishing Group.

Michael, Andrew (2021), "From Tulips to Bitcoin: Why Investment Markets Are Forever Blowing Bubbles", Forbes, 24.5.2021, available at: https://www.forbes.com/uk/advisor/personal-finance/2021/05/24/from-tulips-to-bitcoin-why-investment-markets-are-forever-blowing-bubbles/, accessed on May 13, 2022.

Mullany, Gerry (2013), "China Restricts Banks' Use of Bitcoin", The New York Times, 05.12.2013, available at: http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-usingbitcoin.html, accessed om May 17, 2022.

Nguyen, Tuan (2014), "I bought coffee at the Prague cafe that only accepts bitcoin. Here's what it was like", the Washington Post, 05.11.2014, available at: https://www.washingtonpost.com/news/innovations/wp/2014/11/05/i-bought-coffee-at-theprague-cafe-that-only-accepts-bitcoin-heres-what-it-was-like/, accessed on June 3, 2022.

Pejovich, Svetozar (1990), "The Economics of Property Rights: Towards a Theory of Comparative Systems", Kluwer academic publishers, Boston, U .S.A.

Pick, Leon (2014), "Poland: Bitcoin derivatives are financial instruments, Bitcoin isn't currency", Finance Magnates, 09.07.2014, available at: http://www.financemagnates.com/cryptocurrency/news/poland-bitcoin-derivatives-are-financial-instruments-bitcoin-isnt-currency/, accessed on May 27, 2022.

Prableen, Bajpa (2014), "The 5 Most Important Virtual Currencies Other Than Bitcoin", Investopedia, 10.12.2014, available at: http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-currencies-other-bitcoin.asp, accessed on May 25, 2022.

Popper, Nathaniel (2016), "How China Took Center Stage in Bitcoin's Civil War", The New York Times, 29.06.2016, available at: http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html, accessed on June 3, 2022.

Reingold, Steven C. and Durken, Timothy J., "Bitcoins are not U.S. Dollars: What Does the Rulling in the HashFast Bankruptcy Mean", available at: http://www.jagersmith.com/downloads/pdf/Bitcoins-Are-Not-

US-Dollars.pdf, accessed on May 27, 2022.

Reitman, Rainey (2011), "Bitcoin – a Step Toward Censorship-Resistant Digital Currency", Electronic Frontier Foundation, 20.01.2011, available at: https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant, accessed on June 3, 2022.

Russell, Helen (2015), "No wallet, no worries: Denmark considering cash-free shops", the Guardian, 14.05.2015, available at: https://www.theguardian.com/world/2015/may/14/no-wallet-no-worries-denmark-considering-cash-free-shops, accessed on May 27, 2022.

Scheinert, Christian, (2015), "Virtual currencies, Challenges following their introduction", available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf, accessed on May 27, 2022.

Segal, Ilya and Whinston, Michael D. (2010), "Property Rights", Stanford University, 07.08.2010, available at: http://web.stanford.edu/~isegal/prights.pdf, accessed on June 3, 2022.

Smithin, John N. (1994), "Controversies in Monetary Economics", Edward Elgal Publishing, U.S.A., 1994.

Tange, Alexander (2015), "Denmark proposes cash-free shops to cut retail costs", Reuters, 06.05.2015, available at: http://www.reuters.com/article/denmark-cash-idUSL5N0XX2ZQ20150506, accessed on May 26, 2022.

Tedeschi, Bob (2001), "E-Commerce Report: Seller of Online Currency May Have Been Victim of Fraud", the New York Times, 27.08.2001, available at: http://www.nytimes.com/2001/08/27/business/e-commerce-report-seller-of-online-currency-may-have-been-victim-of-fraud.html?_r=0, accessed on June 3, 2022.

Walker, Herman (1963),"The International Law of Commodity Agreements", Law and Contemporary problems, Duke University.

Woo, David et al. (2013), "Bitcoin: A First Assessment", 05.12.2013, available at: https://ciphrex.com/archive/bofa-bitcoin.pdf, accessed on may 25, 2022.

NDIKIMI I TEKNOLOGJISË NË TË DREJTAT E NJERIUT

M.SC. MARJELA PERI

marielamile@hotmail.com

M.SC. ANXHELA LALAJ

anxhela-lalaj@hotmail.com

Abstrakt

Ky punim analizon në brëndësi të tij elementë të rëndësishëm që lidhen me ndikimin e teknologjisë në të drejtat themelore të njeriut. Të gjithë njerëzit lindin të lirë dhe të barabartë në dinjitet dhe në të drejta. Ata kanë arsye dhe ndërgjegje dhe duhet të sillen ndaj njëri-tjetrit me frymë vëllazërimi. Që nga ky moment shumëi i rëndësishëm i cili daton në vitin 1948 me themelimin e Deklaratës Universale të të Drejtave të Njeriut, njohja dhe respektimi i këtyre të drejtave themelore mori një tjetër kuptim. Zhvillimi i shoqërisë ka sjellë gradualisht zgjerimin e fushës ku përfshihen të drejtat themelore dhe zgjërimin e instancave që shërbejnë për mbrojtjen e tyre.

Fusha e të drejtave themelore përfshin një sërë të drejtash të njohura dhe të integruara në të gjitha sistemet e së drejtës në pjesën më të madhe te shteteve të botës, që tashme gëzojnë mbrojtje ligjore dhe mosrespektimi i tyre shoqërohet me sanksione.

Përparimi i madh që shoqëritë kanë bërë që nga krijimi i Deklaratës Universale të të Drejtave të Njeriut ka ardhur edhe si rrjedhojë i përparimit të teknologjisë e cila ka pasur një implikim të pashmangshëm dhe të thellë në kornizën e të drejtave të njeriut. Rritja dhe ndikimi i teknologjisë ka ndikuar pozitivisht dhe negativisht njëkohësisht, në respektimin dhe mbrojtjen e këtyre të drejtave themelore. Teknologjitë e reja, kanë potencialin për

të dhënë kontribut pozitiv në promovimin dhe mbrojtjen e të drejtave të njerëzve nëpërmjet informimit dhe zgjerimit të njohurive në njohjen dhe respektimin e tyre.

Ajo cka vjen si shqetësim në ditet e sotme është fakti që zhvillimi i këtyre teknologjive ngre pikëpyetje të rëndësishme nëse politikat tona aktuale, sistemet ligjore, dokumentacioni dhe strategjitë e ndërmarra janë të mjaftueshme për të zbutur rreziqet e cënimit dhe këqpërdorimit të të të drejtave themelore të njeriut që janë baza e krijimit dhe funksionimit të një shoqërie demokratike dhe te pavarur.

Adresimi i këtyre sfidave kërkon përpjekje për të siguruar që zhvillimi dhe zbatimi i teknologjive të reja respekton dhe promovon të drejtat e njeriut.

Fjalë kyce: Të drejta themelore, teknologjia, media socilale, jeta private, sanksione.

Abstract

This paper analyzes in its interior important elements related to the impact of technology on fundamental human rights. All people are born free and equal in dignity and rights. They have reason and conscience, and they have to behave towards each other with a spirit of fraternity. From this very important moment, which dates back to 1948 with the establishment of the Universal Declaration of Human Rights, the recognition and respect of these fundamental rights took on another meaning. The development of society has gradually brought about an expansion of the scope where fundamental rights are included and an expansion of the instances that serve to protect them.

The area of human rights includes a set of rights recognized and integrated into all systems of law in most countries of the world, which currently are protected by legal provisions and infringing these rights is accompanied by sanctions.

The great progress that societies have made since the establishment of the Universal Declaration of Human Rights has also come because of the advancement of technology, which has had an inevitable and profound implication in the human rights framework. The growth and impact of technology has positively and negatively influenced, at the same time, respecting, and protection of these fundamental rights. New technologies have the potential to make a positive contribution to the promotion and protection of people's rights through information and the expansion of knowledge over these rights and the obligation to respect.

What comes as a concern nowadays is the fact that the development of these technologies raises important questions about whether our current policies, legal systems, documentation, and strategies undertaken are sufficient to mitigate the risks of violation and misuse of fundamental human rights that underlie the establishment and functioning of a democratic and independent society.

Addressing these challenges requires efforts to ensure that the development and implementation of new technologies respects and promotes human rights.

Keywords: Fundamental right, technology, social media, private life, sanctions.

1. Të drejtat themelore të njeriut

Të drejtat themelore të njeriut janë ato të drejta të cilat mbrohen me ligj dhe janë të barabarta për të gjithë njerzit. Këtë e gjejmë në nenin e parë të Deklaratës Universale të të Drejtave të Njeriut, ku të gjithë njerëzit lindin të lirë e të barabartë në dinjitet e të drejta 1. Ndër të drejtat themelore mund të përmendim të drejatat e lirisë individuale, të drejtën e jetës, të drejtën për jetë private dhe familjare, e drejta e shprehjes, e drejta e fesë etj.

Të drejtat themelore parashikohen shprehimisht dhe mbrohen si nga legjislacioni ndërkombetar dhe nga legjislacioni brendshëm. Gjithkush ka të drejtë për përdorimin e mjeteve juridike të frytshme para gjykatave kompetente kombëtare për veprimet me të cilat shkelen të drejtat themelore të garantuara nga kushtetuta ose ligjet.2

Konventa Europiane e të Drejtave të Njeriut është instrumenti kryesor pas Deklaratës Universale që përcakton të drejtat dhe liritë themelore të cilat kurrë nuk mund të shkelen nga Shtetet. Këto përfshijnë të drejtën për jetë ose ndalimin e torturës, të drejtën për liri dhe siguri ose të drejtën për respektimin e jetës private dhe familjare. Ajo siguron një bazë të përbashkët ligjore që lejon të kuptuarit e njëjtë të të drejtave të njeriut për njerëzit që nuk ndajnë të njëjtat tradita politike, ligjore ose shoqërore.

Po ti referohemi legjislacionit shqipëtar të drejtat themelore të individëve parashikohen ne Kushtetutë që është dhe ligji themeltar i shteti. Pra të drejtat

1 Neni 1 i Deklaratës Universale të të Drejtave të Njeriut në 1948

2 Deklarata Universale e të Drejtave të Njeriut, neni 8.

themelore mbrohen me ligj dhe shkelja e tyre sjell aplikimin e sanksioneve të ndryshme parashikuar në ligjet e posacme.

Në ditët e sotme ashtu si në cdo aspekt bota po përballet dhe me impaktin që ka sjellë zhvillimi i teknologjisë në respektimin dhe në mbrojtjen e të drejtave themelore të njeriut. Zhvillimi i teknologjise ka sjell një impakt pozitiv dhe negativ në njohjen dhe respektimin e te ketyre të drejtave dhe një nga të drejtat më të prekura si pasoje e zhvillimit teknologjik është e drejta për jetë private dhe ndikimi i teknologjisë në të dhënat personale të gjithesecilit prej nesh.3 E drejta për jetë private ashtu sic e kemi përmendur dhe në brëndësi të punimit, analizohet paralelisht me të drejtën e shprehjes. Dimë që neni 10 i Konventës Europiane parashikon se: "Çdokush ka të drejtën e lirisë së shprehjes. Kjo e drejtë përfshin lirinë e mendimit dhe lirinë për të marrë ose për të dhënë informacione ose ide pa ndërhyrjen e autoriteteve publike dhe pa marrë parasysh kufijtë". Nga ana tjetër, dimë që nenet 6 dhe 8 të po kësaj konvente sjellin rregullime të të drejtave të tjera të lidhura me individin, duke siguruar në këtë mënyrë një lloj balance midis këtyre dy të drejtave themelore që qëndrojnë përballë njëra tjetrës. Konventa, por dhe aktet e tjera ligjore parashikojnë shprehimisht të drejtat themelore dhe rastet eksplicite të kufizimit të tyre. Paragrafi i dytë i nenit 10 shprehet se: "Ushtrimi i këtyre lirive… mund t'u nënshtrohet disa formaliteteve, kushteve, kufizimeve ose sanksioneve të parashikuara nga ligji dhe që, në një shoqëri demokratike, përbëjnë masa të nevojshe, për ruajtjen e shëndetit ose të moralit, për mbrojtjen e dinjitetit ose të të drejtave të të tjerëve. Në përputhje me lirinë e shprehjes, çdo organ mediatik ka të drejtën që të publikojë informacione duke përfshirë fakte, rrethana, vlerësime apo mendimet e lira të individëve ndaj një çështjeje me interes publik por nga ana tjetër ka detyrimin që të ruajë dhe të respektoj të drejtën për jetë private. Është pikërisht kalimi i këtij kufiri midis lirisë së shprehjes dhe të drejtës për jetë private që përbën dhe cënimin e kësaj të drejte themelore si pasoje e zhvillimit të teknologjisë në ditët e sotëme. Është e rëndësishme të përmendet se ky funksion i medias televizive dhe medias online por edhe i të gjitha aplikacioneve dhe rrjeteve sociale duhet të ushtrohet pa dallime dhe pa diskriminime në shoqërinë e lirë demokratike por duke respektuar të drejtat dhe liritë themelore të të gjithë individëve pa përjashtim. Ka më shumë se 10 vjet që roli dhe funksioni i

3 Konventa Europiane e të Drejtave të Njeriut, neni 8.
Çdokush ka të drejtën e respektimit të jetës së tij private dhe familjare, banesës dhe korrespondencës së tij. Autoriteti publik nuk mund të ndërhyjë në ushtrimin e kësaj të drejte, përveçse në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes të sigurisë publike, për mbrojtjen e rendit publik, shëndetit ose moralit ose për mbrojtjen e të drejtave dhe lirive të të tjerëve.

medias është përsosur duke përqasur dhe teknologjitë e reja dhe duke sjellë forma të ndryshme të operimit të saj si media në internet apo media sociale.

2. E drejta për jete private dhe e drejta e shprehjes.

Neni 8 dhe neni 10: Ekuilibrimi i të Drejtës për Jetë Private me të Drejtën e Lirisë së Shprehjes

Një nga rastet më të dukshme, kur ngrihet çështja e ekuilbrit midis të drejtës të lirisë së shprehjes dhe të drejtave të tjera, është rasti kur ushtrimi i lirisë së shprehjes nga një person, ndikon në të drejtën e jetës private të një personi tjetër të garantuar në nenin 8 të Konventës.

Në krye të herës, Gjykata ka ndërmarrë një interpretim të zgjeruar të nocionit të jetës private, në vend të një interpretimi më të ngushtë, e cila do të kufizonte fushëveprimin e konceptit tradicional të privatësisë. Koncepti i "jetës private" është më i ngjashëm me konceptin e autonomisë personale. Si rezultat i kësaj, qëllimit të jetës private nuk mund ti vendoset një kufi që për të qenë në përputhje me sigurinë juridike. Në çështjen e Linguistikës Belge 4, Gjykata u shpreh se jeta private përfshin të drejtën për të jetuar jetën e dikujt pa pasur ndërhyrje arbitrare. Gjykata shkoi edhe më tej duke thënë se "Respekti për jetën private duhet të përfshijë në një shkallë të caktuar të drejtën për të krijuar dhe zhvilluar marrëdhënie me qeniet e tjera njerëzore" 5. Gjithsesi, kuptimi i plotë i nenit 8 nuk do të thotë, se ai mbron çdo veprim që një person mund të kërkojë në marrëdhëniet me qeniet e tjera njerëzore për të krijuar dhe zhvilluar marrëdhënie të tilla. Neni 8 i Konventes Europiane i te drejtave te njeriut 6 parashtron të drejtat e sakta që i garantohen një individi nga Shteti, të drejtën për respektimin e jetës private, atë familjare, banesës dhe korrespondencës. Gjithashtu qartëson faktin që këto të drejta nuk janë absolute në kuadrin që i bën ato të pranueshme për autoritetet publike që të ndërhyjnë në të drejtat e ketij neni në rrethana të caktuara. Ky nen tregon gjithashtu rrethanat në të cilat autoritetet publike mund të ndërhyjnë në mënyrë ligjore në të drejtat e parashtruara në Nenin 8/1: vetëm ndërhyrjet që janë në përputhje me ligjin dhe të nevojshme në një shoqëri demokratike në ndjekje të një ose më shumë synimeve legjitime të renditura në kete nen do të konsiderohen si kufizime të pranueshme nga Shteti për

4 Shih Çështja "Në Lidhje me Aspekte të Caktuara të Ligjeve mbi Përdorimin e Gjuhëve në Fushën e Arsimit në Belgjikë" k Belgjikës',

5 Shih Niemietz k Gjermanisë, Ap. No. 13710/88, vendim i 16 dhjetorit 1992, paragrafi 29.

6 Konventa Europiane e te Drejtave te njeriut, neni 8 .

të drejtat e individit. Në përcaktimin nëse masat e marra nga Shteti janë në përputhje me Nenin 8, Shtetit i jepet një shkallë te caktuar lirie, e njohur si liria e vlerësimit.

Për shembull, kjo nuk do të garantojë marrëdhënie ndërpersonale të një fushe veprimi të gjerë dhe të papërcaktuar, që s'mund të ketë lidhje të mundshme të drejtpërdrejta midis veprimit ose mosveprimit të një Shteti dhe jetës private të një personi" 7. Objekti kryesor i nenit 8 është të mbrojë individët ndaj ndërhyrjeve arbitrare nga shteti në ndonjë nga katër fushat e mbrojtura.

Por së pari, individi i dëmtuar duhet të tregojë se: 1.Të drejtat e tij/saj sipas nenit 8 kanë qenë të përfshira. A përfshihet rasti në fushëveprimin e një prej të drejtave të garantuara në nenin 8? Nëse jo, neni 8 nuk zbatohet. 2. Shteti ka ndërhyrë në këto të drejta – a janë veprimet e shtetit të mjaftueshme për të derivuar në një ndërhyrje në jetën private të një personi apo një nga fushat e tjera të garantuara? Nëse ka pasur një ndërhyrje e tillë, ajo nuk mund të jetë e justifikuar nëse Shteti nuk mund të tregojë se ndërhyrja ishte në përputhje me ligjin. Në lidhje me nenin 10, ashtu si u diskutua më sipër, ligji në fjalë duhet të jetë mjaftueshëm i sigurt në formulimin dhe parashikimin e pasojave të tij. Ajo duhet gjithashtu të jetë në dispozicion të publikut. Ndërhyrja ndjek një ose më shumë nga qëllimet legjitime të përcaktuara në nenin 8/2. Ndërhyrja ishte e nevojshme në një shoqëri demokratike. Kjo do të thotë se ndërhyrja duhet të plotësojë një nevojë të ngutshme sociale dhe duhet të jetë në përpjesëtim me qëllimin legjitim të ndjekjur. Qëllimet legjitime në fjalë janë të parashikuara në paragrafin e dytë të nenit 8, përkatësisht: Siguria kombëtare, siguria publike ose mirëqenia ekonomike e një vendi. Mbrojtja e rendit dhe parandalimi i krimit. Mbrojtja e shëndetit dhe moralit. Mbrojta e të drejtave dhe lirive të të tjerëve.

- Ndërveprimi me Nenin 10 lidhet me faktin se një nga fushat në të cilat parashikohen detyrimet pozitive të një Shteti sipas nenit 8, është kontrolli i duhur i autoriteteve publike në ushtrimin e të drejtës së lirisë së shprehjes nga ana e individëve, duke pasur parasysh dispozitën e qartë të nenit 10 se ushtrimi i lirisë së shprehjes përmban detyrime dhe përgjegjësi. Kështu, për shembull, mungesa e një mjeti në lidhje me publikimin e informacionit që lidhet me çështje private mund të përbëjë mungesë të respektimit të jetës private. 8

7 Friend dhe të Tjerët k Mbretërisë së Bashkuar, Ap. Nr. 16072/06, 27809/08, DA 24 nëntor 2009

8 Schüssel k Austrisë, Ap. Nr. 40409/98, vendim i 21 shkurtit 2002.

Gjyqtarët e gjykatave vendase duhet të kenë parasysh vendosjen e ekuilibrit të duhur midis të drejtave të nenit 8 dhe nenit 10 me qëllim respektimin e këtyre dy të drejtave, ku asnjëra prej të cilave nuk prevalon ndaj tjetrës.9

Asambleja Parlamentare e Këshillit të Evropës ka deklaruar se: "Asambleja riafirmon rëndësinë e të drejtës së gjithësecilit për privatësi, dhe të drejtës për lirinë e shprehjes, si dy të drejta themelore për një shoqëri demokratike. Këto të drejta nuk janë as absolute dhe nuk mund të renditen në mënyrë hierarkike, për sa kohë që ato kanë një rëndësi të njëjtë." 10

Jane disa parime, të cilat janë të zbatueshme kur kërkohet vendosja e një ekuilibri mes nenit 10 dhe nenit 8. Së pari, në mënyrë që neni 8 të gjejë zbatim, një "sulm mbi dinjitetit e një personi duhet të arrijë një nivel të caktuar ashpërsie dhe të bëhet në mënyrë të tillë që të shkaktojë dëme në gëzimin personal të të drejtës për respektimin e jetës private".11

Liria e shprehjes përbën një nga themelet bazë të një shoqërie demokratike, se ajo është e zbatushme jo vetëm për "informacione" ose 'ide' që janë marrë në mënyrën e duhur ose konsiderohen si të padëmshme apo si çështje të paanshmërisë, por edhe për ata që fyejnë, trondisin ose shqetësojnë, dhe se çdo përjashtim për lirinë e shprehjes duhet të interpretohet në mënyrë rigoroze dhe nevoja për çdo kufizim duhet të përcaktohet në mënyrë bindëse. Pra liria e shprehjes si një e drejtë themelore duhet te trajtohet gjithmnë në raport të barabartë me të drejtën për jetë private në mënyrë që të mos kemi cënim të kësaj të fundit.

3. Zhvillimi i teknologjisë dhe ndikimi i saj në të drejtat themelore

Zhvillimi i medias online, i rrjeteve socioale si Facebook, Instagram, Twiter dhe i shumë portaleve të tjera janë platformat më të reja të shpikura nga njerëzimi, funksioni i parë i të cilëve është plotësimi i nevojave të publikut për komunikim, informimin, ndërveprim, socializim, etj.

Nga njëra anë zhvillimi i teknologjisë dhe përsosmëria e mediave dhe e aplikacioneve online që ka sjellë ky zhvillim, ndihmojnë në lirinë e shprehjes dhe përhapjen e informacionit duke bërë të mundur njohjen dhe

9 Von Hannover k Gjermansë, Ap. Nr. 59320/00, vendim i 24 qershorit 2004, paragrafi 58.

10 Rezoluta 1165 (1998) e Asamblesë së Parlamentit të Këshillit të Europës, paragrafi 10.

11 Shih Delfi AS k Estonisë, Ap. Nr. 64569/09, vendim i Dhomës së Madhe i 16 qershorit 2015, paragrafi 137

marrjen e informacioneve në rrugë më të shkurtër dhe më të shpejtë por nga ana tjetër zhvillimi i vrullshëm e i teknologjisë përbën një risk potencial për respektimin e jetës private, si edhe shkeljen e të dhënave personale. Doktrina ka pranuar dhe legjislacioni ka rregulluar se, "Liria e shprehjes nuk është një e drejtë absolute" ndërsa jurisprudenca e GJEDNJ - së ka theksuar gjithmonë rolin e kësaj të drejte në raport me respektimin e të drejtave të tjera. Disa nga të drejtat e tjera që kufizojnë zbatimin e lirisë së shprehjes, përveç të drejtës për respektimin e jetës private dhe familjare janë: e drejta për një proces të rregullt gjyqësor; e drejta e pronës; infrastrukturës së shërbimit të medias; rregullimet e profesionit të gazetarit; mosdiskriminimi; e drejta e jetës; apo e drejta për tu organizuar.

Nga njëra anë zhvillimi i teknologjise ndihmon në informimin e individëve, në lirinë e shprehjes dhe në përsosmërinë e medias si një ndër mjetet kryesore të informimit në shoqërinë tonë, por nga ana tjetër ritmi me të cilin po zhvillohet teknologjia përbën një risk potencial për respektimin e jetës private si dhe shkeljen e të dhënave personale.

Teknologjia mund të ndikojë pozitivisht në përgjigjen tonë ndaj sfidave globale po në disa aspekte ndikon negativisht, ne respektimin e disa të drejtave themelore nëse mekanizmat e përdorur për mbrojtjen e këtyre të drejtave nuk janë të mjaftueshëm dhe efektiv për parandalimin e këtij rreziku.

Zhvillimi i teknologjise ka ardhur si rrjedhojë i plotësimit të nevojave që ka pasur shoqëria njerëzore, por bashkë me plotësimin e këtyre nevojave ky zhvillim ka sjellë dhe një sfidë të madhe në lidhje me rregullimin ligjor për të shmangur cënimin e të drejtave themelore të njeriut.

Kriptimi, anonimiteti dhe mjetet e sigurisë dixhitale mund të përdoren për të mbrojtur sigurinë e grave dhe vajzave në internet, të cilat do të forcojnë të drejtat e njeriut. Mund të përdoret gjithashtu për të mbrojtur mbrojtësit e të drejtave të njeriut që janë duke punuar për çështje të dhunës dhe diskriminimit me bazë gjinore. Interneti lejon që informacioni të transmetohet shumë shpejt nga kudo dhe nga kushdo. Teknologjitë e thjeshta si telefonat inteligjentë të cilët kanë një përdorim të gjerë së fundmi gjithashtu lejojnë që cdo informacion të merret dhe të shpërndahet në botë në kohë reale. Gjithashtu e bën shumë të lehtë për publikun që të informohet dhe ndërgjegjësohet për padrejtësitë dhe ngjarje të ndryshme në botë dhe kjo mund të mobilizojë në mënyrë efektive njerëzit për të mbrojtur të drejtat dhe fushatën e tyre kundër abuzimeve të të drejtave të njeriut ndërsa ato po ndodhin.

Në të njejtën kohë, zhvillimet e shpejta në teknologjitë e ditëve të sotme, ngrejnë pyetje serioze mbi impaktin potencial të të drejtave njerëzore dhe

punën në të ardhmen, dhe po ashtu se kush do të përfitojë apo kush do të humbë nga ky zgjerim.

Për sa më lart, ky zhvillimi ndihmon në informimin e individëve, në lirinë e shprehjes dhe në përsosmërinë e medias si një ndër mjetet kryesore të informimit në shoqërinë tonë por nga ana tjetër ritmi me të cilin po zhvillohet teknologjia përbën një risk potencioal për respektimin e jetës private si dhe shkeljen e të dhënave personale. Mungesa e sigurisë së të dhënave personale dhe përpunimi i të dhënave në mënyrë jo të drejtë dhe të ligjshme përbëjnë dy nga rrisqet e sigurisë së informacionit të përhapur në internet dhe në portalet online.

E drejta për mbrojtje të të dhënave personale bën pjesë tek të drejtat e mbrojtura sipas nenit 8 të KEDNj-së, i cili garanton të drejtën për respektim të jetës private dhe familjare, banesës dhe korrespondencës dhe përcakton kushtet sipas së cilëve lejohen kufizimet e kësaj të drejte.12

Kur flitet për platforma të ndryshme dixhitale, është e zakonshme të dëgjosh për vjedhjen e të dhënave ose për të drejtat e privatësisë. Sot shumë kompani të teknologjisë janë përballur me çështje etike për shkak të keq-trajtimit të të dhënave të përdoruesve.

Legjislacionet e vendeve të ndryshme përfshirë dhe Shqipërinë kanë parashikuar përgjegjësinë rast pas rasti të medias në cenimin e të drejtave të njeriut dhe rastet e kufizimit të këtyre të drejtave, referuar nenit 17 të Kushtetutës 13 dhe nenit 120 të Kodit Penal. 14

---

12 KiE, Konventa Evropiane e të Drejtave të Njeriut, STCE nr. 005, 1950

13 Shih Kushtetuta e Republikës së Shqipërisë neni 17
Kufizime të të drejtave dhe lirive të parashikuara në këtë Kushtetutë mund të vendosen vetëm me ligj për një interes publik ose për mbrojtjen e të drejtave të të tjerëve. Kufizimi duhet të jetë në përpjesëtim me gjendjen që e ka diktuar atë. 2. Këto kufizime nuk mund të cenojnë thelbin e lirive dhe të të drejtave dhe në asnjë rast nuk mund të tejkalojnë kufizimet e parashikuara në Konventën Europiane 9 për të Drejtat e Njeriut.

14 Shih Kodi Penal neni 121
Vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimi ose regjistrimi i fjalëve, fiksimi ose regjistrimi figurave, si dhe ruajtja për publikim i të dhënave që ekspozojnë një aspekt të jetës private të personit, pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.
Shpërndarja, ofrimi për publikim apo publikimi me çdo mjet ose formë të komunikimit publik apo mënyrë tjetër i të dhënave të marra në mënyrën e përcaktuar në paragrafin e parë të këtij neni, dënohet me burgim deri në tre vjet.
Po kjo vepër, kur kryhet ndaj personave të mitur, dënohet me burgim nga një deri në tre vjet. Kur vepra penale kryhet nëpërmjet shfrytëzimit të funksionit shtetëror ose shërbimit publik apo nga personi që disponon këto të dhëna për shkak të detyrës shtetërore apo shërbimit publik, dënohet me burgim nga një deri në tre vjet.

Në një botë që po bëhet në mënyrë drastike gjithnjë e më kritike për teknologjinë, është e rëndësishme të mbani mend atë që na ka dhënë gjithashtu.

4. Jurisprudenca e Gjykates Europiane për të drejtat e njeriut.

Respektimi i jetës private dhe familjare përbën një nga kufizimet më të shpeshta të lirisë së shprehjes. Parashikimet e përgjithshme të kufizimit i gjejmë të shprehura në ligj, zbatimin e tyre në praktikë e gjejmë të konsoliduar në jurisprudencën e gjykatave. Në sistemin Evropian, Gjykata Evropiane e të Drejtave të Njeriut ka shpjeguar në arsyetimet e vendimeve të saj rastet e kufizimit të lirisë së shprehjes në përputhje, si edhe përparësinë që ka respektimi i jetës familjare dhe private.

Në tërësinë e jurisprudencës së saj, GjEDNj-ja ka shqyrtuar temën e mbrojtjes së të dhënave në shumë raste, kryesisht në lidhje me përgjimin e komunikimeveb [15] ,format e ndryshme të survejimit dhe mbrojtjen nga mbajtja e të dhënave nga ana e autoriteteve publike . Gjykata ka qartësuar se neni 8 i KEDNj-së jo vetëm që detyron shtetet që të mos kryejnë veprime të cilat mund të shkelin këtë të drejtë të parashikuar nga Konventa, por i detyron në rrethana të caktuara, të garantojnë në mënyrë aktive respektimin e efektshëm të jetës private dhe familjare.[16] Shumë nga këto çështje do të paraqiten me hollësi në vijim.

Përjashtimisht në çështjen Lingens vs. Austria, Gjykata ka pranuar se në rastet kur aplikanti (ankuesi) është person publik, liria e shprehjes do të ketë përparësi në respektimin e saj, krahasimisht me të drejtën për jetë private që mbrohet nga neni 8 i Konventës Evropiane për të Drejtat e Njeriut.

Megjithëse gjykatat e çdo sistemi, GJEDNJ apo dhe gjykatat kombëtare, praktikën e tyre të konsolidimit në zgjidhjen e konfliktit e zhvillojnë ndërmjet lirisë së shprehjes dhe të drejtës për respektimin e jetës private, zhvillimi i teknologjisë është shpesh më i shpejtë dhe ecën me ritme shumëfish më të larta. Debati mbi raportin e të drejtës për informim dhe jetës private është ngritur vitet e fundit në një standard tjetër, në atë të zbulimit të personalitetit

15 Shih GjEDNj, Malone kundër Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984; GjEDNj, Copland kundër Mbretërisë së Bashkuar, nr. 62617/00, 3 prill 2007.

16 Shih GjEDNj, I. kundër Finlandës, nr. 20511/03, 17 korrik 2008; GjEDNj, K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008

dhe evidentimit të karakteristikave, profileve dhe pëlqimeve të individit. [17]

Në çështjet më objekt shpifjen në aspektin penal dhe çështjet e shkaktimit të dëmit nga publikimet ofensive, duhet të krijohet një balancë e drejtë në konfliktin midis dy të drejtave themelore, të cilat meritojnë respekt të barabartë. [18]

Në botën e sotme virtuale të teknologjisë së informacionit rreziku i cenimit të të drejtave të personalitetit nga një publikim ofensiv bëhet gjithnjë e më i vështirë për t'u kontrolluar, për shkak të aksesit universal në përmbajtjen e publikimit on-line. Aftësia e pajisjeve të reja dixhitale si kompjuterët apo celularët për të transmetuar informacionin në nivel global, përbën një sfidë për të drejtën e privatësisë.[19] Në kushtet aktuale të pandemisë Covid-19 dhe fuqizimit të rolit ndërlidhës të platformave on-line, platforma e famshme për video konferenca në internet Zoom Video Communications, po përballet me një padi class action të paraqitur para gjykatës federale të Kalifornisë për shpërndarjen dhe cenimin e të dhënave të përdoruesve me kompani si Facebook pa pëlqimin e subjekteve të të dhënave.

Gjykata në vendimin e saj themelor në çështjen "Handyside kundër Mbretërisë së Bashkuar", [20] pohoi se: "Liria e shprehjes "gjen zbatim jo vetëm për "informacionin" ose "idetë" që pranohen pozitivisht apo konsiderohen si të padëmshme ose çështje për t'u shpërfillur, por edhe për ato që ofendojnë, tronditin ose shqetësojnë shtetin ose çdo grup të popullsisë. Të tilla janë kërkesat e pluralizmit, tolerancës dhe mendjes së hapur, pa të cilat nuk ka një "shoqëri demokratike.

Në çështjen "Lingens kundër Austrisë", 1986, gjykata mbështeti hapur lirinë për të kritikuar qeverinë duke u shprehur se: "Është detyra e shtypit të japë informacion dhe ide mbi çështjet politike ashtu si mbi ato në fushat e tjera të interesit publik. Jo vetëm shtypi ka detyrën të japë informacione të tilla dhe ide: edhe publiku ka një të drejtë për t'i marrë ato". Duke qenë se liria që po diskutojmë i referohet dhënies si të informacionit edhe ideve, bëhet i rëndësishëm dallimi që ka përcaktuar Gjykata në këtë fazë të hershme. Duke bërë një dallim të qartë midis informacionit (fakteve) dhe mendimeve (gjykimet mbi vlerat), Gjykata është shprehur se ekzistenca e fakteve mund

17 Revista avokatia nr 28

18 Shih Vendimi i GJEDNJ "Axel Springer AG k. Gjermanisë", aplikimi nr.39954/08, datë 7.2.2012.

19 Shih vendim I GJEDNJ jacqueline D. Lipton, "Digital Multi-Media and the Limits of Privacy Laë", 42 Case Ë. Res. J.

20 Shih vendimin e GJEDNJ "Handyside kundër Mbretërisë së Bashkuar",

të demonstrohet, kurse e vërteta e vlerave nuk është e prekshme si provë.

Ndërsa mendimet janë pikëpamje ose vlerësime personale të një ngjarjeje ose situate dhe nuk janë të prekshme si prova për të qenë të vërteta ose të gënjeshtërta, faktet e parashtruara mbi të cilat mendimet bazohen, mund të jenë të mundshme për t'u vërtetuar si të vërteta apo të gënjeshtra.

Po në të njëjtën mënyrë Gjykata në çështjen "Dalban" u shpreh: "Do të ishte e papranueshme për një gazetar që t'i hiqet e drejta për të shprehur gjykime subjektive kritike, përderisa ai ose ajo do të mund ta vërtetojë të vërtetën që thotë".[21]

Lidhur me të drejtën e privatësisë në dimensionet e sotme të modernizimit të mjeteve të përhapjes së informacionit, GJEDNJ-ja ka konstatuar se interneti ndryshon nga media e shkruar dhe rreziku që ai shkakton ndaj të drejtës për privatësi të garantuar nga neni 8 i KEDNJ është sigurisht më i lartë. Në çështjen "K.U k. Finlandës" GJEDNJ ka theksuar: "Megjithëse liria e shprehjes dhe konfidencialiteti i komunikimit janë konsiderata parësore dhe përdoruesit e shërbimeit të Internetit duhet të kenë një garanci se do të respektohet privatësia e tyre dhe liria e shprehjes, një garanci e tillë nuk mund të jetë absolute dhe i nënshtrohet kufizimeve legjitime, të tilla si parandalimi i krimit ose mbrojtja e të drejtave dhe lirive të të tjerëve".[22]

Gjithashtu, në çështjen "Delfi kundër Estonisë [23]" Dhoma e Madhe e Gjykatës Evropiane për të Drejtat e Njeriut, ka theksuar funksionin që kryen shtypi në një shoqëri demokratike. Megjithëse shtypi nuk duhet t'i kapërcejë disa kufij të caktuar, veçanërisht për sa i përket reputacionit dhe të drejtave të të tjerëve dhe nevojës për të parandaluar zbulimin e informacioneve konfidenciale, detyra e tij sidoqoftë është të përcjellë – në pajtueshmëri me detyrimet dhe përgjegjësitë e veta – informacione dhe ide mbi të gjitha çështjet e interesit publik

Duke marrë në konsideratë "detyrat dhe përgjegjësitë" e gazetarit, impakti potencial mbi mediumin në fjalë është faktor i rëndësishëm dhe njihet botërisht që mediat audiovizuale shpesh kanë efekt më të menjëhershëm dhe më të fuqishëm sesa mediat e shtypura[24]

Gjykata ka vendosur që "dënimi i një gazetari për ndihmë në përhapjen e deklaratave të dhëna nga një person tjetër gjatë një interviste do të pengonte

21 Shih Vendimin e GJEDNJ, "Dalban kundër Rumanisë", viti 1999

22 Shih Vendimi i GJEDNJ "K.U k. Finlandës", aplikimi nr.2872/02, datë 2.3.2009

23 Shih Vendimin e GJEDNJ Delfi kunder Estonise

24 Shih Vendimin Purcell dhe të Tjerë kundër Irlandës, nr. 15404/89

në mënyrë serioze kontributin e shtypit në diskutimin e çështjeve të interesit publik dhe nuk duhet të mendohet në qoftë se nuk ka arsye veçanërisht të forta për ta bërë këtë".[25]

Gjykata përsërit më tej që e drejta e mbrojtjes së reputacionit është e drejtë e cila është e mbrojtur nga Neni 8 i Konventës si pjesë e së drejtës për respektim të jetës private megjithatë, në mënyrë që të hyjë në lojë Neni 8, një sulm kundër reputacionit të një personi duhet të arrijë një shkallë të caktuar të të qenit serioz dhe të jetë kryer në një mënyrë të atillë që të shkaktojë paragjykim ndaj gëzimit personal të të drejtës për respekt ndaj jetës private.[26]

Konkluzione dhe rekomandime

Ashtu sic e kemi trajtuar dhe në brëndësi të punimit zhvillimi i teknologjise ka pasur një impakt sa pozitiv po aq dhe negativ në respektimin e disa prej të drejtave themelore të njeriut. Duke pasur parasysh që në ditët e sotme kemi një zhvillim të gjerë të medias online dhe të rrjeteve sociale të cilat përdoren në masë nga e gjithë shoqëria, shteti shqipëtar dhe institucionet ligjbërëse duhet të marrin masa dhe të miratojnë rregulla që lidhen me shpërndarjen e informacionit nëpërmijet internetit. Në shumicen e kohës në internet përhapen informacione të cilat nuk janë të vërteta dhe që cënojnë jetën private dhe të dhënat personale të cdo indidvidi. Dua të sjell në vëmëndje në këtë pikë ngjarjen e ndodhur ne muajin Maj në Librazhd që u quajt "rasti i Librazhdit" ku u trajtua rasti dhe historia e një vajze 20-vjecare e cila u filmua me të dashurin nga familjarët e burrit dhe pasoi me përhapjen e videove në të gjitha portalet dhe mediat onlin. Videot që u përhapën në kohë reale në të gjitha portalet online kishin në përmbajtje të tyre pamjen e vajzës të cilës i bëhej një gjyq publik për veprimet e saj, nga të gjithë "gjyqëtarët" e fisit të bashkëshortit të vet dhe askush nuk mendoi as për një minutë që kësaj vajze po i cënonin jetën private si një ndër të drejtat themelore që asaj i garantohet nga ligji. Përhapja e këtyre videove ku ekspozonin vajzën në fjalë dhe gjithë portretin e saj një një gjëndje të degraduar thjesht për disa klikime më shumë pa menduar për asnjë cast për të drejtat e saj, solli si rrjedhoj cënimin e integritetit psikologjik dhe cënimin e të drejtës për jetë private. Kjo video qarkulloi për disa ditë rresht në portale dhe nuk pati asnjë masë për parandalimin e përhapjes së saj dhe ky nuk ka qënë i vetëmi rast i këtij lloji cka tregon se tashmë këmbana e alarmit po paralajmëron se masat që duhen të merren ndaj këtyre rasteve janë urgjente dhe të domosdoshme.

25 Shih Vendimin Thoma kundër Luksemburgut,

26 Shih Vendimin A. kundër Norvegjisë, nr. 28070/06.

Legjislacioni penal shqipëtar parashikon ne nenin 121 të Kodit Penal nderhyrjet e padrejta në jetën private por ky sanksionim i bërë në legjislacionin penal nuk ka sjell parandalimin e e cënimit të jetës private dhe të dhënave personale nga përhapja e informacioneve në mediat dhe portalet online.

Legjislacioni shqiptar për mediat audiovizuale parashikon rregullimet të detajuara në lidhje me reklamimin apo fushatat zgjedhore dhe me qëllime marketingu, por ndërsa televizioni është zëvendësuar ndjeshëm nga rrjetet sociale, Shqipëria duhet të miratojë rregulla që lidhen me shpërndarjen e informacionit nëpërmjet internetit.

Autoriteti i medias audiovizive përcjell informacion të vazhdueshëm në lidhje me respektimin e të dhënave personale nga ana e medias audiovizive, por ende nuk ka një autoritet mbikqyrës në lidhje me median online apo shërbimet online për përhapjen e informacioneve te cilat përbejne shkelje te te drejtave themelore. Pra duhet te ekzistoj një autoritet mbikqyrës për parandalimin e perhapjes së ketyre informacioneve, të cfarëdolloji qofshin ato nga të gjitha mediat online apo dhe nga rrjetet e ndryshme sociale.

Ajo cka është dhe me alarmante është fakti se në shumicën e rasteve askush nuk mban përgjegjsi penale për shkeljen e të drejtave themelore dhe mbi te gjitha për shkeljen e jetës private nga përhapja e informacioneve të ndryshme ne mediat televizive apo kudo në mediat online.

Monitorimi i mediave dhe portaleve online duhet të ketë një rregullim të posacëm duke bërë të mundur parandalimin e përhapjes së informacioneve të papërshtatëshme dhe atyre të cilat cënojnë jetën private dhe familjare të gjithësecilit prej nesh por edhe sigurinë kombëtare të cdo shteti.

Literatura

- Deklarta Universale e te Drejtave te Njeriut 1948.
- Konventa Europiane e Te Drejtave te Njeriut 1950.
- Kushtetuta e Republikës së Shqipërisë, mirtuar me ligjin nr.8417 datë 21.10. 1998.
- Kodi Penal i Republikës së Shqipërisë, miratuar me ligjin nr.7895, datë 27.1.1995.

Jurisprudencë

-Jurisprudenca e Gjykatës së Strasburgut botimi i katërt.

- Vendime të Gjykatës Evropiane të të Drejtave të Njeriut për çështjet: Çështja "Në Lidhje me Aspekte të Caktuara të Ligjeve mbi Përdorimin e Gjuhëve në Fushën e Arsimit në Belgjikë" k Belgjikës', Niemietz k Gjermanisë, Ap. No. 13710/88, vendim i 16 dhjetorit 1992, paragrafi 29; Friend dhe të Tjerët k Mbretërisë së Bashkuar, Ap. Nr. 16072/06, 27809/08, DA 24 nëntor 2009; Schüssel k Austrisë, Ap. Nr. 40409/98, vendim i 21 shkurtit 2002; Von Hannover k Gjermansë, Ap. Nr. 59320/00, vendim i 24 qershorit 2004, paragrafi 58; Delfi AS k Estonisë, Ap. Nr. 64569/09, vendim i Dhomës së Madhe i 16 qershorit 2015, paragrafi 137; GjEDNj, Malone kundër Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984; GjEDNj, Copland kundër Mbretërisë së Bashkuar, nr. 62617/00, 3 prill 2007; GjEDNj, I. kundër Finlandës, nr. 20511/03, 17 korrik 2008; GjEDNj, K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008; Vendimi i GJEDNJ "Axel Springer AG k. Gjermanisë", aplikimi nr.39954/08, datë 7.2.2012; Vendim I GJEDNJ jacqueline D. Lipton, "Digital Multi-Media and the Limits of Privacy Laë", 42 Case Ë. Res. J; Vendimin e GJEDNJ "Handyside kundër Mbretërisë së Bashkuar"; Vendimin e GJEDNJ, "Dalban kundër Rumanisë", viti 1999; Vendimi i GJEDNJ "K.U k. Finlandës", aplikimi nr.2872/02, datë 2.3.2009; Vendimin e GJEDNJ Delfi kunder Estonise; Vendimin Purcell dhe të Tjerë kundër Irlandës, nr. 15404/89; Vendimin Thoma kundër Luksemburgut; Vendimin A. kundër Norvegjisë, nr. 28070/06.

Të tjera

https://comunica.org/com_rights/hamelink.pdf

http://data.europa.eu/eli/reg/2016/679/oj.

https://scholarlycommons.laë.case.edu/cgi/vieëcontent.cgi?article=1244&context=jil.

https://www.idp.al/ëpcontent/uploads/2017/07/Manual_i_s%C3%AB_Drejt%C3%ABs_Evropiane_n%C3%AB_Fush%C3%ABn_e_Mbrojtjes_s%C3%AB_t%C3%AB_Dh%C3%ABnave.pdf

LIDHJA MES TË DREJTAVE TË NJERIUT DHE TEKNOLOGJISË DHE EFEKTI I TYRE NË TË DREJTAT E NJERIUT

MSC. INGRIDA BEHRI MUSTAFA
Studioligjorebehri@gmail.com

MSC. LIRA SPIRO
lira.spiro@unipavaresia.edu.al

Abstrakt

Të drejtat e njeriut sot janë bërë gjithnjë e më komplekse, për shkak të zhvillimit të teknologjisë dhe ndikimit të saj të drejtpërdrejtë. Me zhvillimin e saj, të drejtat e njeriut po bëhen gjithnjë e më të diskutueshme dhe shumë çështje po ngrihen për analizë. Zhvillimet e fundit teknologjike kanë luajtur një rol të madh në rritjen e shumë vendeve, për sa i përket sistemeve ekonomike dhe sociale. Rrjedhimisht, çdokush sot mund ta përdorë lehtësisht internetin në mjetet e tij në mënyra të ndryshme dhe për qëllime të ndryshme. Pikërisht për qëllimin e saj, ne ngremë problemet dhe efektet negative të shkaktuara në të drejtat e njeriut. Kështu, shfaqen dhe nxirren shumë probleme në fushën e të drejtave, në lidhje me mbrojtjen e të dhënave, privatësinë, sigurinë dhe aspekte të tjera. Meqenëse Covid-19 ka shkaktuar mbyllje të gjerë të shkollave dhe distancë fizike, platformat dhe komunikimi në internet u bënë thelbësore për të ruajtur një ndjenjë normaliteti.

Ky punim do të përcaktojë problemet dhe çështjet ligjore brenda aspekteve të të drejtave të njeriut në dritën e zhvillimeve të shpejta teknologjike. Ky punim synon të analizojë dhe identifikojë lidhjen ndërmjet të drejtave të njeriut dhe zhvillimit të teknologjive të reja, duke marrë parasysh çështjet

ligjore dhe etike. Në fund të këtij punimi do të arrijmë të:

- Analizojmë çështjet e mbrojtjes së të dhënave dhe privatësisë;
- Eksplorimit të metodave të mbrojtjes së të dhënave;
- Diskutojmë lidhjen midis zhvillimit të teknologjisë dhe efekteve të saj tek njerëzit dhe të drejtat e tyre.

Fjalët kyçe: të drejtat e njeriut, ligj, teknologji, privatësi, siguri, mbrojtje të të dhënave, etika

Hyrje

Të drejtat e njeriut janë të përcaktuara në ligjet ndërkombëtare dhe vendore. E drejta ndërkombëtare për të drejtat e njeriut kërkon që shtetet kombëtare të respektojnë, mbrojnë dhe përmbushin të drejtat e njeriut dhe të mbështesin parimin se "të gjitha qeniet njerëzore lindin të lirë dhe të barabartë në dinjitet dhe të drejta". Të drejtat e njeriut janë universale, që do të thotë se ato vlejnë për të gjithë. Ato janë të pandashme,[1] të ndërvarura dhe të ndërlidhura, që do të thotë se përmirësimi i një të drejte njerëzore mund të lehtësojë përparimin e të tjerëve. Po kështu, privimi i një të drejte mund të ndikojë negativisht edhe në të drejtat e tjera të njeriut. Ndërsa ndonjëherë ka ndërlidhje komplekse midis të drejtave të ndryshme, qeveritë duhet të sigurojnë që të drejtat e njeriut të gjithsecilit të mbrohen. Një qasje e të drejtave të njeriut ndërton të drejtat e njeriut në të gjitha aspektet e ligjit, zhvillimin e politikave dhe vendimmarrjen.

Kjo e fundit ka rëndësi primare përsa kohë shoqëria njerëzore evoluon dhe zhvillohet me ritme të shpejta. Pjesë e këtij zhvillimi është edhe teknologjia. Zhvillimi i teknologjisë aktualisht është shndërruar në pjesë të pandarë të jetës tonë dhe me efekte të shumta. Sigurisht zhvillimi i teknologjisë ka prekur dhe prek të drejtat e njeriut. Ndaj shtetet dhe organizmat ndërkombëtare që objektin e punës së tyre kanë të drejtat e njeriut, duhet të përfshijnë në qasjet e tyre të zhvillimit të të drejtave të njeriut edhe efektet dhe përdorimin e teknologjive të reja, kjo e fundit ndërkohë gjithnjë e më shumë po zhvillohet ndërkombëtarisht.

Një numër në rritje ekspertësh theksojnë rëndësinë e ligjit të të drejtave

1 Fergus Hunter and Jennifer Duke, ''Not Messing Around': Government Unveils 'World-leading' Regulation of Tech Giants', Sydney Morning Herald (online, 12 December 2019)

të njeriut në analizimin e ndikimit social të teknologjisë.[2] Disa iniciativa ndërkombëtare përdorin të drejtat e njeriut si objektivin kryesor, ose një nga disa prej tyre, përmes të cilave mund të shihet zhvillimi dhe përdorimi i teknologjive të reja. Duke qenë se teknologjitë janë të reja, po zhvillohet edhe zbatimi i të drejtave të njeriut dhe ligjeve të tjera në këtë fushë. Disa nga organizatat ndërkombëtare që mbështesin një qasje të të drejtave të njeriut për zhvillimin dhe përdorimin e teknologjive të reja përfshijnë:[3]

- Mekanizmat e Kombeve të Bashkuara (OKB), si Komisioneri i Lartë i OKB-së për të Drejtat e Njeriut dhe Raportuesit Special për varfërinë ekstreme dhe të drejtat e njeriut, privatësinë dhe lirinë e shprehjes dhe diskriminimin racor;
- Parimet Udhëzuese të OKB-së për Biznesin dhe të Drejtat e Njeriut;
- Organet ndërkombëtare shumëpalëshe, si Organizata për Bashkëpunim dhe Zhvillim Ekonomik (OECD)16 dhe G2017;
- Organizatat joqeveritare dhe të industrisë që punojnë në kryqëzimin e të drejtave të njeriut dhe teknologjive të reja.

Zhvillimet e fundit teknologjike kanë luajtur një rol të madh në rritjen e shumë vendeve, përsa i përket sistemeve ekonomike dhe sociale. Përparimet në telekomunikacion dhe teknologjinë kompjuterike, tani po i lejojnë njerëzit të lidhen lehtësisht dhe lirshëm nëpër kontinente, qoftë për kënaqësi dhe socializim, qoftë për arsye biznesi. Sot, çdokush është në gjendje të marrë informacion pothuajse për çdo gjë, menjëherë, duke përdorur motorët e kërkimit në internet.[4]

Kjo e çon kohën e lirë, biznesin dhe edukimin në një nivel të ri, duke lejuar kryerjen e mësimit në distancë, bizneset e pavarura dhe komunikimin e drejtpërdrejtë me këdo në mbarë botën, duke i bërë përparimet teknologjike një faktor jetik për zhvillimin e mëtejshëm të ekonomive në mbarë botën. Kjo, megjithatë, ngre çështje të reja në fushën e të drejtave të njeriut, në lidhje me mbrojtjen e të dhënave, privatësinë, sigurinë dhe aspekte të tjera. Sipas autorit Ëeeramantry, disiplinat e ligjit dhe të drejtave të njeriut

2 ICCPR; ICESCR; Convention on the Elimination of all Forms of Discrimination Against Women, opened for signature 18 December 1979, 1249 UNTS 13 (entered into force 3 September 1981) ('CEDAW')

3 Office of the High Commissioner of Human Rights, UN Human Rights Business and Human Rights in Technology Project (B-Tech): Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies (November 2019).

4 Kerikmäe, T.; Hamulak, O.; Chochia, A. (2016). A Historical Study of Contemporary Human Rights: Deviation or Extinction? Acta Baltica Historiae et Philosophiae Scientiarum, 4 (2), 98−115

nuk janë në gjendje të vazhdojnë me ndryshimet dhe zhvillimet e shpejta në teknologji. Ndaj shtrohet diskutimi dhe analizimi e rrjedhimisht gjetja e zgjidhjeve për problemin ligjor në fushën e kryqëzimit të të drejtave të njeriut dhe zhvillimit të teknologjisë.[5]

Tërësia e të drejtave qw parashikohen nga Deklarata Universale e tw Drejtave tw Njeriut janë kushtet minimale që lejojnë mbrojtjen e një individi nga cënimet e jashtme, duke garantuar autonominë e tij, sigurinë, mundësinë e shprehjes së lirë të vullnetit dhe sjelljes, arsimimin dhe të ardhurat minimale.[6] Sipas Deklaratës së Asamblesë së Përgjithshme mbi të Drejtën për Zhvillim përcaktohet: "*E drejta për zhvillim është një e drejtë e patjetërsueshme e njeriut, në bazë të së cilës çdo person dhe të gjithë popujt kanë të drejtë të marrin pjesë, të kontribuojnë dhe të gëzojnë zhvillim ekonomik, social, kulturor dhe politik, në të cilin të gjitha të drejtat dhe liritë themelore të njeriut mund të të realizohet plotësisht."*[7]

Studiuesi Ëeeramantry vëren se parimet kryesore të promovimit të së drejtës për zhvillim ekonomik, social, kulturor ose politik me përdorimin e teknologjisë janë si më poshtë:

- "Pjesëmarrje në vendimmarrje për futjen e një teknologjie të re";
- "Kontribut në krijimin e teknologjisë në fjalë";
- "Kënaqësi e zhvillimit që rezulton nga teknologjia".[8]

Zhvillimi i teknologjive të reja të informacionit mund të shihet si përfaqësim i të drejtës për të shpërndarë lirisht informacionin dhe të drejtën për ta marrë lirisht atë, si dhe vetë shfaqja e këtyre teknologjive mund të shihet si një përparim i kërkimit të lirë shkencor. Sipas Afrikhanova, teknologjia moderne e informacionit po ndërmjetëson marrëdhënien midis marrësit të informacionit dhe burimit të tij, gjë që rrit në masë të madhe mundësitë për manipulimin e vetëdijes së përdoruesve të një informacioni të tillë.[9]

---

5 Myers, J. (1998). Human rights and development: Using advanced technology to promote human rights in subSaharan Africa. Case Ë. Res. J. Int'l L., 30, 343.

6 Weeramantry, C. G. (1993).The Impact of Technology on Human Rights. Retrieved from: http://archive.unu.edu/unupress/lecture4.html

7 Kerikmäe, T.; Hoffmann, T.; Chochia, A. (2018). Legal Technology for Law Firms: Determining Roadmaps for Innovation. Croatian International Relations Review, 24

8 Po aty

9 Weeramantry, C. G. (1993). The Impact of Technology on Human Rights. Retrieved from: http://archive.unu.edu/unupress/lecture4.html

Ndikimi i teknologjive të reja në të drejtat kryesore ekonomike, sociale dhe kulturore

Teknologjitë e reja, duke përfshirë teknologjitë dixhitale, kanë potencial të madh dhe implikime të thella për realizimin e të drejtave ekonomike, sociale dhe kulturore, si dhe për të gjitha të drejtat e tjera të njeriut dhe për ndryshimet transformuese të parashikuara nga liderët botërorë në Axhendën 2030 për Zhvillim të Qëndrueshëm[10]. Teknologjitë e reja mund të zgjerojnë me shpejtësi cilësinë dhe aksesin në shumë shërbime dhe produkte thelbësore për realizimin e të drejtave ekonomike, sociale dhe kulturore. Në të njëjtën kohë, ato përfshijnë rreziqe të konsiderueshme në përkeqësimin potencial të boshllëqeve dhe pabarazive ekzistuese dhe krijimin e të rejave. Për më tepër, përfitimet e teknologjive të reja aktualisht nuk shpërndahen në mënyrë të barabartë në të gjithë dhe brenda vendeve. Disa teknologji dixhitale shpesh kanë pasoja negative të paparashikuara.[11]

Me angazhimin e saj qendror për të mos lënë askënd pas, Axhenda 2030 i ka dhënë një shtysë të rëndësishme politike realizimit të të drejtave ekonomike, sociale dhe kulturore dhe përpjekjeve për të trajtuar pabarazinë. Nëse shfrytëzohen dhe shpërndahen në mënyrë të barabartë, teknologjitë e reja mund të lehtësojnë shumë realizimin e të drejtave ekonomike, sociale dhe kulturore dhe të ndihmojnë në sigurimin e arritjes së elementeve të tyre kyçe të disponueshmërisë, përballueshmërisë, aksesueshmërisë dhe cilësisë.[12]

Teknologjitë e reja hapin mundësi për "kapërcim" – duke anashkaluar fazat e ndërmjetme të teknologjisë nëpër të cilat vendet kanë kaluar historikisht gjatë procesit të zhvillimit – të cilat mund të përshpejtojnë ritmin e realizimit progresiv të të drejtave ekonomike, sociale dhe kulturore.[13]

Teknologjitë e reja mund të mbështesin gjithashtu përpjekjet e shteteve për të promovuar të drejtën për pjesëmarrje dhe akses në informacion dhe për të përmirësuar efikasitetin dhe efektivitetin e vendimmarrjes publike, me synimin për të maksimizuar përdorimin e burimeve të disponueshme për realizimin e çështjeve ekonomike, sociale dhe kulturore. Këto teknologji

10 https://www.un.org/sustainabledevelopment/development-agenda/

11 High-level Panel on Digital Cooperation, "The age of digital interdependence: report of the UN Secretary-General's High-level Panel on Digital Cooperation", June 2019, p. 17.

12 International Telecommunication Union, Measuring Digital Development: Facts and Figures 2019 (Geneva, 2019), p. 3–4.

13 International Telecommunication Union, Measuring Digital Development: Facts and Figures 2019 (Geneva, 2019), p. 3–4.

kanë potencial të madh për të avancuar të mirën kolektive të njerëzimit. Në të njëjtën kohë, teknologjitë e reja paraqesin gjithashtu rreziqe të rëndësishme, duke përfshirë respektimin e mbrojtjes së të drejtave të njeriut, të cilat shpesh janë nënprodukte të paqëllimshme të përparimit shkencor dhe teknologjik. Algoritmet shpesh pasqyrojnë dhe riprodhojnë paragjykimet ekzistuese. Mediat sociale mund të keqpërdoren lehtësisht për të përhapur urrejtje. Mbledhja dhe përpunimi i një sasie të madhe të të dhënave personale pa marrë parasysh të drejtën e privatësisë ka implikime të rëndësishme për gëzimin e të drejtave në përgjithësi. Le të ndalemi në disa prej tyre:

E drejta për arsimim

Arsimi është njëkohësisht një e drejtë e njeriut në vetvete dhe një mjet i domosdoshëm për realizimin e të drejtave të tjera të njeriut (E/C.12/1999/10, para. 1). Arsimi dhe të mësuarit janë kritike në përgatitjen e vendeve dhe njerëzve të tyre për ndryshimet që vijnë nga zhvillimi dhe përhapja e përshpejtuar e inovacioneve teknologjike duhet të jetë e kontrolluar, në mënyrë që të maksimizohen përfitimet e tyre duke minimizuar rreziqet e mundshme.[14] Teknologjitë e reja kanë zgjeruar shumë aksesin në arsim dhe mundësitë e të mësuarit, duke e bërë më të lehtë për mësuesit, krijimin e materialeve mësimore dhe duke u mundësuar mënyra të reja njerëzve për të mësuar dhe punuar së bashku..

Përparimi në teknologjitë e reja sjell sfida për sa i përket disponueshmërisë dhe aksesit të së drejtës për arsimim, veçanërisht për njerëzit e varfër dhe më të margjinalizuar. Qasja në përmbajtjen arsimore dhe mundësitë e shpërndara me mjete dixhitale kërkon infrastrukturë fizike dhe mjete ekonomike. Njerëzit që jetojnë në zonat urbane përgjithësisht gëzojnë akses më të mirë dhe më të lirë në energji elektrike, lidhje interneti me brez të gjerë dhe mjete ekonomike për të blerë pajisje të tilla si kompjuterë, tableta dhe telefona inteligjentë, ndërsa ata në zonat e largëta rurale shpesh reduktohen në përdorimin e teknologjive relativisht të vjetruara.[15]

Teknologjitë e reja rrezikojnë gjithashtu përkeqësimin e pabarazive gjinore dhe të tjera. Sipas vlerësimeve të fundit, hendeku gjinor dixhital po rritet me shpejtësi në vendet në zhvillim. Pabarazitë gjinore në aksesin dhe përdorimin e teknologjisë së informacionit dhe komunikimit shpesh pasqyrojnë diskriminimin me të cilin përballen gratë në shoqëri më gjerësisht

14 International Covenant on Economic, Social and Cultural Rights, art. 13.

15 United Nations Conference on Trade and Development, The Role of Science, Technology and Innovation in Ensuring Food Security by 2030 (Geneva, 2017), pp. 21–22.

dhe kanë efektin të kufizojnë më tej aksesin në teknologji dhe mundësitë e paraqitura prej tyre (A/HRC/35/9, parag. 17).[16]

Në mënyrë të ngjashme, fëmijët me aftësi të kufizuara përballen me disa pengesa për të përfituar nga teknologjia e informacionit dhe e komunikimit për t'iu qasur më mirë mundësive arsimore, pasi teknologjitë dhe përmbajtjet mund të kenë nevojë të përshtaten për përdorimin e tyre (A/HRC/32/37, para. 42). Sigurimi i cilësisë së përvojës së të mësuarit në arsimin online është një sfidë tjetër, pasi nxitësi i shpërndarjes së përmbajtjes mund të mposht nevojën për angazhim dhe ndërveprim të nxënësve. Sipas raportuesit special për të drejtën në arsim, kualifikimet dhe certifikatat e marra përmes kurseve të hapura online shpesh nuk kalojnë nëpër procese të mirëfillta vlerësimi. Për më tepër, duke qenë se kurset e hapura në internet shpesh ofrohen nga/ose në partneritet nga sektori privat, është detyrë e qeverive të vendosin politika dhe rregullore të përshtatshme për të siguruar plotësisht pranueshmërinë, përshtatshmërinë dhe cilësinë e arsimit në përputhje me detyrimet e tyre (seksionet VI dhe XII).[17]

Është e nevojshme të sigurohet që sistemi i përgjithshëm arsimor të respektojë plotësisht të drejtën për arsimim dhe që vetë arsimi të drejtohet drejt zhvillimit të plotë të personalitetit njerëzor dhe ndjenjës së dinjitetit të tij.

E drejta për ushqim

Teknologjitë e reja kanë implikime të shumta dhe komplekse për dimensione të ndryshme të sigurisë ushqimore dhe të drejtës për ushqim. Për shembull, bioteknologjia dhe inxhinieria gjenetike, si dhe teknikat për përmirësimin e pjellorisë së tokës, teknologjitë e ujitjes dhe përdorimin e synuar të agrokimikateve, mund të rrisin disponueshmërinë e ushqimit. Teknologjitë e pas-vjeljes dhe agropërpunimit mund të adresojnë aksesin e ushqimit dhe biofortifikimi mund të përmirësojë cilësinë ushqyese të ushqimit. Në të njëjtën kohë, siguria e mundshme dhe implikimet etike të këtyre teknologjive të reja, duke përfshirë biologjinë sintetike, inteligjencën artificiale dhe inxhinierinë e indeve, do të kërkojnë ekzaminim të ngushtë nga perspektiva e të drejtave të njeriut.[18]

16 Po aty.

17 Po aty.

18 Sustainable Development Outlook 2019: Gathering Storms and Silver Linings (United Nations publication, Sales No. E.20.II.A.1), p. 94.

Thatësirat kërcënojnë gjithnjë e më shumë aksesin në ujë për prodhimin e ushqimit dhe përkeqësojnë urinë. Megjithatë, teknologjitë e reja ofrojnë mjetet për të parashikuar dhe zbutur efektet e mundshme negative të thatësirës në prodhimin e ushqimit.[19] Teknologjia e informacionit dhe e komunikimit mund të luajë një rol të rëndësishëm në fuqizimin e fermerëve dhe sipërmarrësve ruralë me akses në informacion në lidhje me inovacionet bujqësore, kushtet e motit, shërbimet financiare dhe çmimet e tregut dhe lidhjen e tyre me blerësit. Telefonat celularë kanë gjithashtu një potencial të madh për të fuqizuar pronarët e vegjël dhe për të promovuar përfshirjen në treg duke u mundësuar atyre të shesin produktet e tyre që prishen në mënyrë më efektive dhe të negociojnë çmime më të mira.[20]

Në të njëjtën kohë, tendencat drejt dixhitalizimit, financimit të tregut ushqimor dhe komodifikimit të ushqimit, të përshpejtuara nga avancimi teknologjik, po riformësojnë thellësisht sistemet e ushqimit dhe kanë një ndikim të rëndësishëm në të drejtën për ushqim. Teknologjia është në qendër të sistemit të ushqimit industrial, i cili fokusohet në maksimizimin e efikasitetit në prodhimin e ushqimit me koston më të ulët të mundshme dhe mbështetet shumë në inputet kimike, duke ndikuar në cilësinë ushqimore dhe shëndetin publik dhe mjedisor (A/71/282, para. 22– 23). Ndërsa farat dhe materialet e tjera gjenetike bimore po dixhitalizohen dhe patentohen nga korporatat globale, shfaqen rreziqe që qasja në njohuritë tradicionale dhe farat e zhvilluara në mënyra të tjera, përfshirë nga popujt indigjenë, mund të minohet. Dixhitalizimi i regjistrimit të tokës dhe të dhënave të lidhura me tokën me teknologjinë *blockchain*[21] mund të sjellë përfitime të rëndësishme në rritjen e transparencës, efikasitetit dhe sigurisë.Megjithatë, teknologjitë e reja duhet të futen me kujdes në mënyrë që të shmangen pasojat e padëshiruara.duke përfshirë transformimin më të lehtë të interesave të tokës në asete financiare spekulative dhe rreziqet e shpronësimit, në veçanti, të komuniteteve rurale nga toka e zotëruar për një kohë të gjatë.[22]

19 Food and Agriculture Organization of the United Nations, The Future of Food and Agriculture: Trends and Challenges (Rome, 2017), p. 54

20 Po aty.

21 Teknologjia Blockchain përdor një bazë të dhënash të përbashkët dhe të decentralizuar që zotërohet pjesërisht nga çdo anëtar i një rrjeti peer-to-peer dhe jo nga një njësi e vetme (p.sh. një bankë ose DMV lokale), siç është rasti i bazës së të dhënave tradicionale dhe të centralizuara. Për më shumë shih: https://pcworld.al/teknologjia-blockchain/

22 Global Netëork for the Right to Food and Nutrition, Right to Food and Nutrition Ëatch: Ëhen Food Becomes Immaterial: Confronting the Digital Age, September 2018.

E drejta për shëndet

Teknologjitë e reja, duke përfshirë teknologjitë dixhitale, luajnë një rol të rëndësishëm në realizimin e të drejtës për shëndet dhe mbulim shëndetësor universal për të gjithë. Teknologjia e informacionit dhe e komunikimit mund të zgjerojë disponueshmërinë dhe aksesin e shërbimeve shëndetësore cilësore. Inteligjenca artificiale dhe të dhënat e mëdha po përdoren për të zhvilluar ilaçe të reja, për të ofruar plane trajtimi të personalizuara dhe për të përmirësuar efikasitetin e ofrimit të kujdesit. Kur teknologjitë e reja projektohen dhe zbatohen në një mënyrë të përgjegjshme, ato ofrojnë potencial për të transformuar shërbimet shëndetësore, për të zgjeruar aksesin në shërbimet parandaluese, diagnostikuese dhe trajtuese, për të ofruar edukim shëndetësor dhe për të zgjeruar njohuritë dhe kërkimin. Pavarësisht përfitimeve të mundshme, teknologjitë e reja si dixhitalizimi në kujdesin shëndetësor, nuk janë gjithmonë të nevojshme ose të përshtatshme në të gjitha rrethanat ose për të gjithë njerëzit. Meqenëse teknologjitë prekin njerëz të ndryshëm në mënyra të ndryshme, dizajnimi dhe aplikimi i teknologjive të reja do të duhet të marrë parasysh kushtet dhe nevojat e veçanta të personave në fjalë dhe kontekstin në të cilin teknologjia do të vendoset, në mënyrë që të mos cenohen të drejtat e zbatueshme dhe cenojnë dinjitetin e personave.[23]

Përdorimi i të dhënave të mëdha dhe inteligjencës artificiale në kontekstin shëndetësor paraqet rreziqe të konsiderueshme për të drejtën e pacientëve për privatësi në lidhje me të dhënat e ndjeshme shëndetësore dhe informacione të tjera personale. Me rritjen e teknologjive të shëndetit të konsumatorit si: teknologjia e veshjes dhe aplikacionet e smartfonëve, krijimi, përpunimi, shkëmbimi, shitja e sasive të mëdha të të dhënave shëndetësore është rritur në mbarë botën (A/71/368, para. 13). Ky trend shoqëron rrezikun e shtuar të zbulimit të paqëllimshëm të të dhënave të ndjeshme të pacientëve në lidhje me shëndetin nga institucionet shëndetësore, por edhe të ndarjes së pajustifikuar me palët e treta. Një shqetësim tjetër është aftësia e inteligjencës artificiale për të konkluduar dhe parashikuar kushte shëndetësore që individët nuk i kanë zbuluar vullnetarisht, gjë që mund të rezultojë në mohimin e sigurimit shëndetësor. Kornizat e politikave për të drejtën për shëndet duhet të mbrojnë të drejtën për privatësi dhe siguri në përdorimin e teknologjive dixhitale të shëndetit si: identifikimi biometrik. Rregullimi i përshtatshëm është gjithashtu i nevojshëm për të garantuar cilësinë dhe sigurinë e produkteve softuerike, pajisjeve dhe aplikacioneve që jo vetëm përdoren në kujdesin

23 The conference report of the Integrated National Information and Communications Technology for Health and Development Forum, August 2016. Available at http://1millionhealthworkers.org/files/2016/09/ICT_REPORT.pdf

parësor shëndetësor, por gjithashtu mund të tregtohen drejtpërdrejt ose të disponohen ndryshe për individët.[24]

E drejta për një standard të përshtatshëm jetese

Më shumë se gjysma e popullsisë së botës sot jeton në zona urbane, një numër që pritet të rritet në 68% deri në vitin 2050. Gjithnjë e më shumë, shumë qytete po shfrytëzojnë fuqinë e teknologjive të reja për të adresuar sfidat e paraqitura nga urbanizimi, për të hartuar dhe menaxhuar ndërveprimet komplekse të energjisë, transportit, ujit dhe mbetjeve si dhe për të avancuar qëllimet e Axhendës së Re Urbane dhe Objektivat e Zhvillimit të Qëndrueshëm për t'i bërë qytetet gjithëpërfshirëse, të sigurta, elastike dhe të qëndrueshme. Përdorimi efektiv dhe i përgjegjshëm i teknologjisë së informacionit dhe komunikimit dhe teknologjive dixhitale mund t'i ndihmojë planifikuesit urbanë dhe banorët të rrisin aksesin e barabartë në shërbimet dhe mundësitë urbane.[25] Përpjekjet e ndërgjegjshme dhe të synuara dhe një proces më i gjerë pjesëmarrës janë të nevojshme për të siguruar që teknologjitë e reja të mbështesin realizimin më të mirë të të drejtave ekonomike, sociale dhe kulturore, të tilla si të drejtat për strehim, ujë dhe kanalizime, për njerëzit më të pafavorizuar. Pa përpjekje të tilla, ekziston rreziku që përpjekjet në lidhje me qytetet inteligjente të mos përqendrohen domosdoshmërisht në përmirësimin e cilësisë së jetës urbane për të gjithë dhe sigurimin e aksesit më të mirë në shërbime cilësore, veçanërisht për njerëzit e varfër dhe të pafavorizuar.[26]

E drejta për të punuar

Vala globale e ndryshimeve teknologjike ka një ndikim të thellë në të ardhmen e vendeve të punës, duke paraqitur si mundësi ashtu edhe sfida për realizimin e të drejtës për punë, përfshirjen e të drejtës për gëzimin e kushteve të drejta dhe të favorshme të punës. Automatizimi dhe teknologjitë e reja po krijojnë mundësi të reja pune, duke eliminuar të tjerat. Robotët dhe automatizimi mund të zvogëlojnë ose eliminojnë detyrat e rrezikshme dhe të kontribuojnë në të drejtën për kushte të sigurta pune. Në të njëjtën

24 Po aty.

25 World Urbanization Prospects: The 2018 Revision (United Nations publication, Sales No. E.20. II.A.1), p. xix.

26 Desiree Fields and Dallas Rogers, "Towards a critical housing studies research agenda on platform real estate", Housing, Theory and Society, 2019, p. 4.

kohë, shumë punëtorë që janë në rrezik të humbasin punën e tyre për shkak të automatizimit dhe robotizimit, mund të detyrohen të pranojnë punë me aftësi më të ulëta dhe me pagë më të ulët. Natyra në ndryshim e vendeve të punës kërkon grupe të reja aftësish, veçanërisht aftësi dixhitale: teknologjitë dixhitale përdoren në të gjitha llojet e punëve, duke përfshirë në sektorë që më parë ishin më pak të lidhur me teknologji të tilla, si bujqësia, shëndetësia dhe ndërtimi.[27] Kur bëhet fjalë për ndikimin e ndryshimeve teknologjike në grupmosha të ndryshme, një sfidë që shfaqet është nevoja për përshtatje dhe rikualifikim dhe zhvendosje të të rriturve, veçanërisht të të moshuarve, të prekur nga ndryshimet teknologjike.[28] Megjithatë, ndërsa platformat e shërbimit dixhital mund të krijojnë mundësi të reja pune dhe të ndihmojnë në stabilizimin e marrëveshjeve joformale të punës, shumë punëtorë në ekonominë e koncerteve përballen me pasiguri më të madhe në situatën e tyre të punës. Marrëveshjet e punësimit të këtij lloji janë shpesh të natyrës së përkohshme dhe përfshijnë punëdhënës të shumtë, duke penguar ose kufizuar aftësinë praktike të punonjësve për të ushtruar të drejtën e tyre për lirinë e shoqërimit, duke përfshirë të drejtën për të formuar dhe bashkuar sindikatat, siç nuk e dinë shumica e punëtorëve në platformat online.[29]

Çështjet e të dhënave dhe privatisë

Një nga aspektet e të drejtave të njeriut që ndikohet nga zhvillimi i teknologjisë është mbrojtja e të dhënave dhe privatësia. Kryerja e transaksioneve financiare duke përdorur internetin, porositja e mallrave dhe shërbimeve, përdorimi i kartave të kreditit, aksesi në burimet private të informacionit, transferimi i thirrjeve telefonike kërkojnë një nivel të përshtatshëm sigurie. Sipas Manral, informacioni konfidencial që transmetohet në internet kalon përmes një numri të caktuar ruterash dhe serverësh përpara se të arrijë në destinacionin e tij.[30] Zakonisht ruterat nuk gjurmojnë rrjedhat e informacionit që kalojnë nëpër to, por ekziston mundësia që informacioni të përgjohet.[31] Për më tepër, informacioni mund të ndryshohet dhe t'i transferohet adresuesit në një formë të modifikuar.

27 European Commission, ICT for Work: Digital Skills in the Workplace (Brussels, 2016).

28 World Health Organization, "Digital technologies: shaping the future of primary health care", 2018, p. 6.

29 Po aty

30 Manral, V., Bhatia, M., Jaeggli, J., & Ëhite, R. (2010). Issues ëith existing cryptographic protection methods for routing protocols (No.RFC 6039).

31 Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust.Computers in human behavior, 28(3), 889-897.

Fatkeqësisht, vetë arkitektura e internetit gjithmonë lë mundësinë që një përdorues i paskrupullt të kryejë veprime të tilla. Ekziston gjithmonë një problem për të zgjedhur midis nivelit të nevojshëm të mbrojtjes dhe efikasitetit të punës në rrjet. Në disa raste, përdoruesit ose konsumatorët e masave të sigurisë mund t'i konsiderojnë ato si masa për të kufizuar aksesin dhe efikasitetin.[32]

Mbajtja private e të dhënave po bëhet gjithnjë e më e vështirë. Përfitimet e *Internet of Things* (IoT)[33] nuk duhet të nënvlerësohen. Ato përfshijnë, për shembull, reduktimin e energjisë duke përdorur sensorë të zgjuar në shtëpi, përdorimin e pajisjeve shtëpiake nga telefoni inteligjent, ruajtjen e informacionit të sigurisë rrugore dhe trafikut, ekzekutimin e diagnostikimeve mjekësore të avancuara, etj.[34] Megjithatë, meqenëse këto teknologji mbledhin dhe ndajnë vëllime të mëdha të dhënash, duhet të ketë sisteme të avancuara dhe të përshtatshme për qëllime të mbrojtjes së të dhënave. Për të siguruar fshehtësinë dhe privatësinë e informacionit të transferuar nëpërmjet internetit, përdoret enkriptimi ose kriptografia, e cila lejon shndërrimin e të dhënave në një formë të koduar, nga e cila është e mundur të nxirret informacioni burimor vetëm nëse ka një çelës. Zhvillimi dhe përdorimi i sistemeve të tilla të mbrojtjes së të dhënave do të jetë gjithashtu i dobishëm për prodhuesit, falë rritjes së besimit nga konsumatori.[35]

Një tjetër zhvillim i kohëve të fundit që duhet diskutuar në dritën e të dhënave dhe privatësisë është "*cloud computing*".[36]Ka shumë përfitime nga përdorimi i cloud[37], kryesisht, kursimi i hapësirës dhe aftësia për të hyrë në të dhënat në cloud nga çdo vegël, në krahasim me ruajtjen e tyre në një pajisje fizike. Për shkak të shqetësimeve për sigurinë e të dhënave, të dhënat e ndjeshme dhe aplikacionet dhe sistemet kritike mbahen ende shpesh në pajisjet fizike, gjë që pengon rritjen e tregut të informatikës cloud.[38] Sfidat

32 Kobie, N. (2015). What is the internet of things? Retrieved from: https://www.theguardian.com/technology/2015/may/06/What-is-the-internet-of-things-google

33 https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

34 Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30.

35 Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30.

36 Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms. In MIPRO, 2011 Proceedings of the 34th International Convention (pp. 1468-1473).IEEE.

37 Cloud computing mund të quhet "cloud" dhe është "shpërndarja e burimeve kompjuterike sipas kërkesës - gjithçka nga aplikacionet tek qendrat e të dhënave - përmes internetit mbi bazën e pagesës për përdorim"

38 Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 1(2011), 1-11

kryesore të sigurimit të kompjuterit cloud, të emërtuara nga Chen dhe Zhao, qëndrojnë në fushën e mbrojtjes së informacionit personal dhe të biznesit të përdoruesit, ndërkohë që ndahen të dhënat në të njëjtën kohë dhe është me rëndësi të madhe përdorimi i sistemeve të tilla që do përcaktonin se cili informacion mund të zbulohet dhe kujt mund t'i zbulohet, në mënyrë që të ruhet funksionaliteti i cloud, duke mbrojtur të dhënat e ndjeshme të përdoruesit.[39] Problemet që lindin nga siguria e transferimit të informacionit gjatë punës në rrjetet kompjuterike mund të përkufizohen si më poshtë:[40]

- Përgjimi i informacionit - ruhet integriteti i informacionit, por cenohet konfidencialiteti i tij;
- Modifikimi i informacionit - mesazhi origjinal ndryshohet ose zëvendësohet plotësisht nga një tjetër dhe i dërgohet adresuesit;
- Zëvendësimi i autorësisë së informacionit;
- Përgjimi i mesazhit me tërheqjen e tij.

Këto probleme mund të kenë pasoja të rënda.[41] Prandaj, mund të konkludohet se, në përputhje me problemet elistuara në diskutimin e çështjeve të sigurisë, termi "siguri" në fushën e mbrojtjes së të dhënave duhet të kombinojë karakteristikat e mëposhtme të ndryshme të një sistemi të sigurimit:[42]

1. Autentifikimi: procesi i njohjes së përdoruesit të sistemit dhe dhënies së të drejtave dhe kompetencave të caktuara. Sa herë që bëhet fjalë për shkallën apo cilësinë e vërtetimit, kjo duhet kuptuar si shkalla e sigurisë së sistemit nga sulmet e palëve të treta ndaj këtyre fuqive.
2. Integriteti: një gjendje e të dhënave në të cilën ato ruajnë përmbajtjen e tyre informative dhe interpretimin e paqartë në kushte të ndikimeve të ndryshme. Në veçanti, në rastin e transmetimit të të dhënave, integriteti mund të shihet si identiteti i dërguar dhe i marrë.
3. Fshehtësia: parandalimi i aksesit të paautorizuar në informacion. Në rastin e transmetimit të të dhënave, ky term duhet të kuptohet si

39 Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647- 651).IEEE.

40 Huang, R. W., Gui, X. L., Yu, S., & Zhuang, W. (2011). Privacy-preserving computable encryption scheme of cloud computing. Jisuanji Xuebao(Chinese Journal of Computers), 34(12), 2391-2402

41 Lloyd, I. (2017). Information technology law. Oxford University Press

42 Theohary, C. A. (2011). Terrorist use of the internet: Information operations in cyberspace. DIANE Publishing.

parandalimi i përgjimit të informacionit.[43]

Konkluzione dhe rekomandime

Në këtë punim, u parashtruan disa nga të drejtat e njeriut përballë sfidave dhe efekteve të zhvillimit të teknologjive të reja. Këto nga ana tjetër identifikojnë një sërë veprimesh që duhe ndërmarrë për të shfrytëzuar mundësitë e teknologjive të reja për realizimin e të drejtave ekonomike, sociale dhe kulturore, duke adresuar njëkohësisht rreziqet e mundshme. Midis tyre, kërkohet Shteteve dhe, sipas rastit, të kompanive private dhe palëve të tjera të interesuara:

- Njohja plotësisht e nevojës për të mbrojtur dhe përforcuar të gjitha të drejtat e njeriut në zhvillimin, përdorimin dhe qeverisjen e teknologjive të reja si objektivin e tyre qendror, dhe garantojnë respektimin dhe zbatimin e barabartë të të gjitha të drejtave të njeriut online dhe offline;
- Miratimi i masave legjislative, duke përfshirë masat në lidhje me aktivitetet e sektorit privat, në mënyrë që teknologjitë e reja të kontribuojnë në gëzimin e plotë të të drejtave të njeriut nga të gjithë, duke përfshirë të drejtat ekonomike, sociale dhe kulturore, dhe të parandalohen ndikimet negative në të drejtat e njeriut ;
- Investimi në të drejtën për mbrojtje sociale për të krijuar qëndrueshmëri ndaj ndryshimeve dhe paqëndrueshmërisë, duke përfshirë ato të shkaktuara nga ndryshimet teknologjike, dhe për të mbrojtur të drejtat e punës në të gjitha format e punësimit;
- Sigurimi i pjesëmarrjes së të gjitha palëve të interesuara në vendimet për zhvillimin dhe vendosjen e teknologjive të reja dhe kërkon shpjegim adekuat të vendimeve të mbështetura nga inteligjenca artificiale, veçanërisht në sektorin publik;
- Kryerja sistematikisht e kujdesit të duhur për të drejtat e njeriut gjatë gjithë ciklit jetësor të sistemeve të bazuara në teknologjitë e reja, veçanërisht sistemet e inteligjencës artificiale, që mund të kenë një ndikim të rëndësishëm në gëzimin e të drejtave të njeriut;
- Krijimi i kornizave dhe mekanizmave të përshtatshëm ligjorë për të siguruar llogaridhënie të plotë në kontekstin e përdorimit të teknologjive të reja, duke përfshirë rishikimin dhe vlerësimin e boshllëqeve në sistemet ligjore kombëtare, krijimin e mekanizmave

43 Po aty.

mbikëqyrës, aty ku është e nevojshme, si dhe vënien në dispozicion të rrugëve për korrigjimin e dëmit shkaktuar nga teknologjitë e reja;

- Trajtimi i diskriminimit dhe paragjykimit në zhvillimin dhe përdorimin e teknologjive të reja, veçanërisht në drejtim të aksesit në produkte dhe shërbime që janë thelbësore përgëzimin e të drejtave ekonomike, sociale dhe kulturore;

Biblografia

- Fergus Hunter and Jennifer Duke, ‘’Not Messing Around’: Government Unveils ‘World-leading’ Regulation of Tech Giants’, Sydney Morning Herald (online, 12 December 2019);
- ICCPR; ICESCR; Convention on the Elimination of all Forms of Discrimination Against Ëomen, opened for signature 18 December 1979, 1249 UNTS 13 (entered into force 3 September 1981) (‘CEDAW’);
- Office of the High Commissioner of Human Rights, UN Human Rights Business and Human Rights in Technology Project (B-Tech): Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies (November 2019).
- Kerikmäe, T.; Hamulak, O.; Chochia, A. (2016). A Historical Study of Contemporary Human Rights: Deviation or Extinction? Acta Baltica Historiae et Philosophiae Scientiarum, 4 (2), 98−115;
- Myers, J. (1998). Human rights and development: Using advanced technology to promote human rights in subSaharan Africa. Case W. Res. J. Int’l L., 30, 343;
- Weeramantry, C. G. (1993).The Impact of Technology on Human Rights;
- Kerikmäe, T.; Hoffmann, T.; Chochia, A. (2018). Legal Technology for Law Firms: Determining Roadmaps for Innovation. Croatian International Relations Review;
- Weeramantry, C. G. (1993). The Impact of Technology on Human Rights.
- High-level Panel on Digital Cooperation, “The age of digital interdependence: report of the UN Secretary-General’s High-level Panel on Digital Cooperation”, June 2019, p. 17.

- International Telecommunication Union, Measuring Digital Development: Facts and Figures 2019 (Geneva, 2019), pp. 3–4.
- International Covenant on Economic, Social and Cultural Rights, art. 13.
- United Nations Conference on Trade and Development, The Role of Science, Technology and Innovation in Ensuring Food Security by 2030 (Geneva, 2017), p. 21–22.
- Sustainable Development Outlook 2019: Gathering Storms and Silver Linings (United Nations publication, Sales No. E.20.II.A.1), p. 94.
- Food and Agriculture Organization of the United Nations, The Future of Food and Agriculture: Trends and Challenges (Rome, 2017), p. 54
- European Commission, ICT for Work: Digital Skills in the Ëorkplace (Brussels, 2016).
- World Health Organization, "Digital technologies: shaping the future of primary health care", 2018, p. 6.
- Manral, V., Bhatia, M., Jaeggli, J., & Ëhite, R. (2010).Issues ëith existing cryptographic protection methods for routing protocols (No. RFC 6039).
- Ëu, K. Ë., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 28(3), 889-897.
- Kobie, N. (2015). What is the internet of things?
- Weber, R. H. (2010). Internet of Things–Neë security and privacy challenges. Computer laë & security review, 26(1), 23-30.
- Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms.In MIPRO, 2011 Proceedings of the 34th International Convention (p. 1468-1473)
- Evans, D. (2011). The internet of things: Hoë the next evolution of the internet is changing everything. CISCO ëhite paper, 1(2011), 1-11
- Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647- 651);
- Huang, R. Ë., Gui, X. L., Yu, S., & Zhuang, W. (2011). Privacy-

preserving computable encryption scheme of cloud computing. Jisuanji Xuebao(Chinese Journal of Computers), 34(12), 2391-2402;

- Lloyd, I. (2017). Information technology law. Oxford University Press;
- Theohary, C. A. (2011). Terrorist use of the internet: Information operations in cyberspace. DIANE Publishing;
- Global Network for the Right to Food and Nutrition, Right to Food and Nutrition Watch: When Food Becomes Immaterial: Confronting the Digital Age, September 2018;
- The conference report of the Integrated National Information and Communications Technology for Health and Development Forum, August 2016;
- World Urbanization Prospects: The 2018 Revision (United Nations publication, Sales No. E.20.II.A.1);
- Desiree Fields and Dallas Rogers, "Towards a critical housing studies research agenda on platform real estate", Housing, Theory and Society, 2019, p. 4;
- Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30;
- Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms.In MIPRO, 2011 Proceedings of the 34th International Convention (pp. 1468-1473);
- Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 1(2011), p.1-11
- Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647- 651).
- Huang, R. W., Gui, X. L., Yu, S., & Zhuang, Ë. (2011). Privacy-preserving computable encryption scheme of cloud computing. Jisuanji Xuebao(Chinese Journal of Computers), 34(12), 2391-2402;
- Lloyd, I. (2017). Information technology laë. Oxford University Press;

Website:

http://1millionhealthëorkers.org/files/2016/09/ICT_REPORT.pdf

http://archive.unu.edu/unupress/lecture4.html

https://www.un.org/sustainabledevelopment/development-agenda/

https://www.theguardian.com/technology/2015/may/06/ëhat-is-the-internet-of-things-google

https://pcworld.al/teknologjia-blockchain/

SHPËRNDARJA KOMPJUTERIKE E MATERIALEVE PRO GENOCIDIT OSE KRIMEVE KUNDËR NJERËZIMIT

ELSA MIHA[1]

ARMAND GURAKUQI[2]

Abstrakt

Genocidi dhe krimet kundër njerëzimit përfaqësojnë dy nga format më ekstreme të padrejtësive njerëzore që synojnë shkatërrimin tërësisht apo pjesërisht të një grupi nacional, etnik, racial, fetar ose të lidhur mbi bindje politike apo ideologjike. Këto fenomene kanë gjetur shtrirje në periudha të ndryshme të historisë, duke u shoqëruar me humbje masive të jetëve të anëtarëve të grupimeve të mësipërme.

Në vazhdimësi komuniteti ndërkombëtar ka reaguar ndaj llojeve të mësipërme të veprave penale, duke krijuar mekanizma ligjorë dhe institucionale për penalizimin e njëherësh për parandalimin e tyre. Një nga qëndrimet e rëndësishme ndërkombëtare është miratimi i "Protokollit Shtesë të Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike". Nëpërmjet këtij dokumenti është synuar, ndër të tjera, saknionimi jo vetëm i genocidit dhe krimeve kundër njerëzimit por edhe i mbështetjes së tyre me anë të zhvillimeve teknologjike.

Republika e Shqipërisë, në vijim të detyrimeve të marra përsipër përmes nënshkrimit të protokollit të mësipërm, ka shtuar disa dispozita penale, ndër

1 Prokurore në Prokurorinë pranë Gjykatës së Shkallës së pare, Tiranë.

2 Prokuror në Prokurorinë pranë Gjykatës së Shkallës së pare, Tiranë.

të cilat është edhe "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit". Studimi i kësaj norme ligjore paraqet rëndësi me qëllim për të analizuar elementet e figurës së veprës penale dhe raportin e saj me dispozitën përkatëse të protokollit të lartpërmendur. Njëkohësisht vlerësohet e nevojshme të trajtohet edhe përgjegjësia penale për konsumimin e veprës penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit" në kuadër të lirisë së shprehjes së individit.

Fjalë kyçe: Shpërndarja kompjuterike, genocidi, krime kundër njerëzimit, liria e shprehjes.

Hyrje

Për shkak të përmasave të rënda të pasojave genocidit, Asambleja e Përgjithshme e Kombeve të Bashkuara, në vitin 1948, ka theksuar qëndrimin se genocidi është një krim sipas ligjit ndërkombëtar, në kundërshtim me frymën dhe qëllimet e Kombeve të Bashkuara dhe i dënuar nga bota e civilizuar.[3] Nevoja për të parandaluar dhe dënuar këtë trajtë agresioni ndaj komuniteteve të ndryshme shërbeu si bazë për miratimin në atë vit të "Konventës mbi Parandalimin dhe Dënimin e Krimit të Genocidit", dokument i cili ka shërbyer për ndërtimin e një reagimi të konsoliduar kundër kësaj figure krimi. Vëmëndje e lartë i është kushtuar në arenën ndërkombëtare edhe krimeve kundër njerëzimit,[4] të cilat për nga rëndesa e pasojave, ashtu si genocidi, përfshihen në grupin e veprave penale më të rrezikshme për shoqërinë.

Bashkëpunimi ndërkombëtar për të penalizuar figurat e mësipërme të veprave penale ka qenë i vazhdueshëm. Kështu ndër masat e para të marra mund të përmendet krijimi dhe funksionimi i Gjykatës Ushtarake Ndërkombëtare e ngritur bazuar në "Kartën e Gjykatës Ushtarake

3 Shih preambulën e Konventës mbi Parandalimin dhe Dënimin e Krimit të Genocidit. I disponueshëm në Doc.1_Convention on the Prevention and Punishment of the Crime of Genocide.pdf.

4 Në nenin 74 të Kodit Penal të Republikës së Shqipërisë "Krimet kundër njerëzimit" parashikohet: "Vrasjet, zhdukja me forcë, shfarosjet, kthimi në skllevër, internimet dhe dëbimet, si dhe çdo lloj torture ose dhune tjetër njerëzore, të kryera, sipas një plani konkret të paramenduar, ose në mënyrë sistematike, kundër një grupi të popullsisë civile, për motive politike, ideologjike, raciale, etnike e fetare dënohen jo më pak se pesëmbëdhjetë vjet ose me burgim të përjetshëm".

Ndërkombëtare"[5] të vitit 1945 ndërmjet Kombeve të Bashkuara.[6] Duke pasuar përpjekjet e vazhdueshme në këtë drejtim një tjetër hap i rëndësishëm është formimi i Gjykatës Ndërkombëtare Penale me Statutin e Romës të vitit 1998.

Ndërkohë shoqëria ka përfituar nga mundësitë e shumta të ofruara nga shkencat informatike. Rrjeti është i pasur me programe kompjuterike që mund të shfrytëzohen për të transmetuar edhe informacionet më të ndërlikuara nga njëri cep i globit në tjetrin. Por zhvillimet e shpejta teknologjike kanë ofruar mundësi edhe për zgjerimin e aktiviteteve të paligjshme. Anonimati, shpejtësia dhe mungesa e kufijve territorialë janë disa prej tipareve të teknologjisë së informacionit, që lehtësojnë ndjeshëm kryerjen e veprave të ndryshme penale.

Komuniteti ndërkombëtar ka vlerësuar të nevojshme që veç sanksionimit të genocidit dhe krimeve kundër njerëzimit, të reagojë edhe ndaj sjelljeve që konsistojnë në përkrahjen apo justifikimin e tyre, për më shumë kur këto qëndrime realizohen nëpërmjet sistemeve kompjuterike. Për këtë arsye në janar të vitit 2003 është hapur për nënshkrim "Protokolli Shtesë i Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike".[7] Në këtë dokument u nënvizua qëndrimi se shprehja e mohimit, minizimit të konsiderueshëm, miratimit ose justifikimit të genocidit dhe krimeve kundër njerëzimit fyen kujtimin e atyre personave që kanë qenë viktima të një fatkeqësie dhe të të afërmve të tyre.[8]

Miratimi i "Protokollit Shtesë të Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike" ishte masa e duhur që duhej të ndërmerrej për të luftuar këtë kategori të veprimtarisë kriminale të kryer në rrjet. Parashikimet e "protokollit shtesë" janë të karakterit detyrues. Për të përmbushur këto detyrime shtetet palë jo vetëm duhet të aktivizojnë legjislacionin përkatës

5 E quajtur ndryshe "Karta e Nurembergut", e cila është pjesë integrale e "Marrëveshjes së Londrës të vitit 1945".

6 Shih The Charter and Judgment of the Nürnberg Tribunal – History and Analysis: Memorandum submitted by the Secretary-General, 89.

7 Ratifikuar me ligjin nr. 9262, datë 29.7.2004. I disponueshëm në https://qbz.gov.al/eli/ligj/2004/07/29/9262/1e7b3c04-3e6b-445f-a14f-db75f2f5714f;q=9262.

8 Shih "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", faqe 7, prg.39. European Treaty Series - No. 189. I disponueshëm në https://rm.coe.int/16800d37ae.

por duhet gjithashtu të sigurojnë zbatimin efektiv të tij.[9]

Figurat e veprave penale të përfshira në Kodin Penal të Republikës së Shqipërisë në zbatim të detyrimeve të marra përsipër me ratifikimin e "Protokollit shtesë" kanë të përbashkët përdorimin e sistemeve kompjuterike si një nga komponentët e anës objektive të figurës së veprës penale. Por nuk është kjo rrethanë ajo që është vlerësuar primare në pozicionimin e dispozitave penale në strukturën e Kodit Penal shqiptar. Radha e këtyre normave në kod është përcaktuar bazuar në objektin e figurave të veprave penale, duke i përshirë ato në kreun apo seksionin e posaçëm të kodit, që mbron të njëjtin objekt. Kështu vepra penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit", e parashikuar nga neni 74/a i K.P. është radhitur në kreun e parë të pjesës së posaçme të kodit "Krime kundër Njerëzimit". Objekt i këtij kreu janë marrëdhëniet juridike të parashikuara për të garantuar, nga veprimet dhe mosveprimet kriminale, jetën dhe shëndetin e individëve që i përkasin komuniteteve të ndryshme. Së pari mbrohen personat që janë pjesë e një grupi nacional, etnik, racial apo fetar si dhe integriteti tërësor i këtyre grupeve.[10] Gjithashtu merret në mbrojtje jeta dhe shëndeti i anëtarëve të një grupi të popullsisë civile që është objekt i sulmeve të paramenduara për shkak të motiveve politike, ideologjike, raciale, etnike e fetare.[11] I njëjti objekt garantohet edhe nga neni 74/a i K.P. "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit". Bazuar në këtë arsyetim është përcaktuar në Kodin Penal shqiptar edhe pozicioni i dispozitave të tjera të "Protokollit shtesë".

1. "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit" [12]

Objekti i figurës së veprës penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit[13]" u trajtua më lart në këtë punim. Por lidhur me këtë element duhet shtuar se mohimi,

9 Po aty.

10 Të mbrojtura nga neni 73 i Kodit Penal "Genocidi".

11 Të mbrojtura nga neni 74 i Kodit Penal "Krimet kundër njerëzimit".

12 Neni 74/a i Kodit Penal të Republikës së Shqipërisë "Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve, që mohojnë, minimizojnë, në mënyrë të ndjeshme, miratojnë ose justifikojnë akte, që përbëjnë gjenocid ose krim kundër njerëzimit, dënohet me burgim tre deri në gjashtë vjet".

13 Shih nenin 74/a të Ligjit nr.7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", I përditësuar.

minizimi i konsiderueshëm, miratimi ose justifikimi i genocidit dhe krimeve kundër njerëzimit, veç cënimit të jetës dhe shëndetit, fyen kujtimin e atyre personave që kanë qenë viktima të një fatkeqësie dhe të të afërmve të tyre. Përfundimisht kërcënon edhe dinjitetin e komunitetit njerëzor.[14]

Një nga elementet kryesorë të anës objektive të veprës penale është "publikimi" i materialeve pro genocidit apo krimeve kundër njerëzimit. Thjesht posedimi apo shpërndarja e kufizuar e këtyre materialeve nuk plotëson kushtin objektiv të kërkuar nga dispozita penale. Në të dy shprehjet "ofrimi në publik" ose "shpërndarja e qëllimshme publikut" legjislatori ka përsëritur termin "publik", me të cilin do të kuptohet tërësia e njerëzve të një vendi, të një qyteti etj..., të cilëve u bëhet e njohur diçka; populli; tërësia e njerëzve në një shfaqje, në një miting.[15] Përzgjedhja e kësaj fjale nga ligjvënësi nënkupton që përhapja e materialeve duhet të jetë masive pra të ketë shtrirje të gjërë. Përhapja publike mund të realizohet edhe në grupet "chat" të komunikimit apo grupet e lajmeve edhe në rast se pjesëmarrja në këto mënyra komunikimi mund të kërkojë masa sigurie si fjalëkalimi.[16] Një qëndrim i tillë konfirmohet edhe në raportin shpjegues të "Protokollit shtesë" ku theksohet se fjala "publikut" e bën të qartë që komunikimet private dalin jashtë qëllimit të parashikimit të nenit 3 të këtij dokumenti.[17]

Nje tjetër komponent i anës objektive është përdorimi i sistemeve kompjuterike. "Sistem kompjuterik" do të thotë çdo lloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi, kryejnë procesime automatike të të dhënave.[18] Nga pikëpamja teknike dhënia e komandës që do të iniciojë procesin e transmetimit të materialeve realizohet në një pajisje të vetme kompjuterike. Por nisur nga natyra publike që duhet të plotësojë shpërndarja e materialeve

14 Shih "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning arela the criminalisation of acts of a racist and xenophobic nature committed through computer systems", faqe 7, prg.39. European Treaty Series - No. 189. I disponueshëm në https://rm.coe.int/16800d37ae.

15 Publik: I disponueshëm në https://fjalorthi.com/publik; **PUBLIK** m: 1. Tërësia e njerëzve të një vendi, të një qyteti etj., të cilëve u bëhet e njohur diçka; masa e gjerë e popullit, popull. 2. Tërësia e njerëzve të mbledhur diku për të parë a për të dëgjuar diçka, për të ndjekur një shfaqje, për të zhvilluar një miting etj. Publik i gjerë (i shumtë, i ngritur, i gjallë). Duartrokitjet (thirrjet) e publikut. I disponueshëm në www.fjalori.shkenca.org .

16 Shih "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", faqe 6, prg.31. European Treaty Series - No. 189. I disponueshëm në https://rm.coe.int/16800d37ae.

17 Po aty, prg.29.

18 Shih nenin 1 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.

është e përshtatshme të pranohet se ajo nuk mund të konsumohet me anë të një pajisjeve të vetme madje as edhe me një numër të kufizuar pajisjesh. Ky proces mund të përmbushet nëpërmjet një grupi të ndërlidhur ose pajisjesh të lidhura, të cilat janë aksesueshme dhe që duhet të jenë të aksesueshme nga publiku.

Një nga pikat që mund të paraqesin diskutime juridike në lidhje me nenin 75/a të K.P. është përmbajtja e materialeve që shpërndahen. Sipas kësaj dispozite të dhënat që përhapen duhet të jenë të tilla që të 1) mohojnë; 2) minimizojnë, në mënyrë të ndjeshme; 3) miratojnë; ose 4) justifikojnë akte, që përbëjnë genocid ose krim kundër njerëzimit. Vlerësimi i ekzistencës ose jo të këtyre elementëve përbërës të normës penale nevojitet të kryhet në disa hapa. Kështu së pari duhet të përcaktohet nëse faktet që shpërndahen nga i dyshuari përbëjnë ose jo genocid ose krime kundër njerëzimit. Në rastin kur konfirmohet ekzistenca e njërit prej këtyre krimeve të rënda hapi pasues do të jetë analiza e qëndrimit që mban i dyshuari ndaj tyre, pra nëse i mohon, minimizon ndjeshëm ose përkrah apo justifikon ato.

Për të konkluduar nëse materialet e shpërndara përbëjnë ose jo genocid ose krime kundër njerëzimit fillimisht duhet të konfirmohet nëse ato, pra të dhënat e ofruara publikut, janë kualifikuar si të tilla nga një vendim gjyqësor i formës së prerë. Në nenin 75/a të K.P. nuk kërkohet ekzistenca e një disponimi gjyqësor përfundimtar mbi praninë e genocidit ose krimeve kundër njerëzimit. Ndërkohë në "Prokollin shtesë" është parashikuar që materialet e shpërndara duhet të jenë pranuar si genocid ose krime kundër njerëzimit, sipas të drejtave ndërkombëtare dhe të njohura si të tilla me vendime të formës të prerë dhe të detyrueshme të Gjykatës Ndërkombëtare Ushtarake, të krijuara nga Marrëveshja e Londrës e 8 prillit 1945 ose të ndonjë gjykate tjetër ndërkombëtare, të krijuar me instrumentet përkatëse ndërkombëtare, juridiksioni i të cilave është njohur nga shtetet palë.[19] Parashikimi i nenit 6 të "Protokollit shtesë" synon të bëjë të qartë që faktet për të cilat saktësia historike është vendosur nuk mund të mohohen, të minizohen gjërësisht, të aprovohen apo justifikohen me qëllim që të mbështeten këto teori dhe ide të neveritshme.[20]

---

19 Shih nenin 6, pika 1 të "Protokollit Shtesë të Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike", ratifikuar me ligjin nr. 9262, datë 29.7.2004. I disponueshëm në https://qbz.gov.al/eli/ligj/2004/07/29/9262/1e7b3c04-3e6b-445f-a14f-db75f2f5714f;q=9262

20 Shih "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", faqe 7, prg.41. European Treaty Series - No. 189. I disponueshëm në https://rm.coe.int/16800d37ae.

Konstatohet se ligjvënësi shqiptar ka zgjedhur të mos përfshijë në nenin 75/a të Kodit Penal të gjithë rrethanat e përcaktuara në nenin 6, pika 1 të "Protokollit shtesë", konkretisht vendimin gjyqësor ndërkombëtar të formës së prerë mbi kualifikimin e fakteve të shpërndara si genocid apo krime kundër njerëzimit. Një miratim i tillë i dispozitës zgjeron mundësinë për gjykatat dhe prokuroritë shqiptare për të kualifikuar sipas nenit 75/a të K.P. edhe rastet kur janë publikuar materiale të vlerësuara si konsumim i neneve 73 "Genocidi" dhe 74 "Krimet kundër njerëzimit" të K.P. edhe me vendim gjyqësor të formës së prerë të brendshëm. Por vlerësohet se në çdo rast ekzistenca paraprake e një vendimi gjyqësor, të ekzekutueshëm, mbi praninë e krimeve të mësipërme, është një kusht i domosdoshëm, mungesa e të cilit passjell edhe mungesën e konsumimit të anës objektive të figurës së veprës penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit".

Në vijim të analizës së elementevë të figurës së veprës penale të parashikuar nga neni 75/a i K.P. nevojitet të trajtohet qëndrimi i të dyshuarit të veprës penale ndaj materialeve të publikuara lidhur me genocidin apo krimet kundër njerëzimit. Sipas dispozitës autori i shpërndarjes duhet të prezantojë qëndrime që mohojnë, minimizojnë në mënyrë të ndjeshme, miratojnë ose justifikojnë akte, që përbëjnë genocid ose krim kundër njerëzimit.

Mohimi mund të shprehet në trajta të ndryshme që mund të konsistojë në mohimin tërësor të një ngjarje që përbën genocid apo krim kundër njerëzimit ose dhe mohimin e vetë klasifikimit të tyre si të tilla. Miratimi i këtyre ngjarjeve përfaqëson një pozicionim të qartë të të dyshuarit në favor të tyre siç mund të jetë nxitja për përsëritjen e krimeve të tilla, vlerësimi pozitiv i tyre etj. Minimizimi i genocidit apo krimeve të luftës mund të konsistojë në reduktimin e përmasave të vërteta të fakteve kriminale, ndërsa justifikimi mund të shprehet nëpërmjet paraqitjes së analizave me synimin për të lehtësuar rrethanat dhe arsyet e realizimit të tyre.

Mohimi, minimizimi, miratimi ose justifikimi përfaqësojnë një komponent të anës objektive të figurës së veprës penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit", të cilat realizohen me qëllimin final për të cënuar objektin e veprës penale. Duke shprehur qëndrime përkrahëse ndaj genocidit autori i veprës penale synon të nxisë kryerjen e veprimeve që rrezikojnë jetën dhe shëndetin e personave që janë pjesë e një grupi nacional, etnik, racial apo fetar si dhe integritetin tërësor të këtyre grupeve. Kur materialet e shpërndara mbështesin krimet kundër njerëzimit synohet të stimulohen sulme të paramenduara ndaj jetës dhe

shëndetit të anëtarëve të një grupi të popullsisë civile për shkak të motiveve politike, ideologjike, raciale, etnike e fetare.

Lidhur me formën e materialeve të shpërndara është e vlefshme të merret në konsideratë qëndrimi i mbajtur nga Gjykata Evropiane e të Drejtave të Njeriut në çështjen Leroy kundër Francës ku është theksuar se edhe një material viziv, siç ishte një vizatim, mund të përfaqësojë një të dhënë që konstituon përhapje racizmi, ksenofobie, genocidi apo krimesh lufte.[21] Nisur nga ky qëndrim vlerësohet se materiali i shpërndarë mund të jetë në forma të ndryshme, si tekste, video, audio etj..., të përshtatshme për t'u përhapur nëpërmjet sistemeve kompjuterike.

Në "Protokollin shtesë" edhe lidhur me dispozitën "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit", parashikohet se një shtet palë mund të kërkojë që mohimi ose minimizimi i konsiderueshëm i përmendur në paragrafin e parë të këtij neni të jetë kryer për të nxitur urrejtjen, diskriminimin ose dhunën kundër një individi ose grupi individësh, bazuar mbi racën, ngjyrën prejardhjen, origjinën kombëtare ose etnike si dhe fenë, nëse përdoret si pretekst për një nga këta faktorë.[22] Një parashikim i tillë nuk është përthithur në nenin përkatës të Kodit Penal shqiptar, në të cilin penalizohet shpërndarja e materialeve raciste ose ksenofobike edhe kur ato nuk nxisin dhunë apo urrejtje. Vlerësohet se një qëndrim i tillë i ligjvënësit shqiptar, në kushtet kur norma e protokollit ia ka besuar vullnetit të shteteve nënshkruese, është shumë i përshtatshëm pasi garanton një mbrojtje më të gjërë të të drejtave të individit të një komuniteti të caktuar.

Përgjegjësia penale për nenin 75/a të K.P. në raport me lirinë e shprehjes

2. Ekzistenca e përgjegjësisë penale për shpërndarjen e materialeve që përkrahin genocidin apo krimet kundër njerëzimit, është e nevojshme të analizohet duke u ballafaquar edhe në raport me lirinë e shprehjes. Në Kushtetutën e Republikës së Shqipërisë parashikohet që liria e shprehjes

21 Çështja Leroy kundër Francës. no. 36109/03, 2 October 2008. I disponueshëm në Leroy v. France (coe.int)

22 Shih nenin 3, pika 2 të "Protokollit Shtesë të Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike", ratifikuar me ligjin nr. 9262, datë 29.7.2004. https://qbz.gov.al/eli/ligj/2004/07/29/9262/1e7b3c04-3e6b-445f-a14f-db75f2f5714f;q=9262.

është e garantuar.[23] Kjo e drejtë garantohet edhe në nenin 10 të Konventës Evropiane për të Drejtat e Njeriut.[24] Bazuar në detyrimin për respektimin e lirisë së shprehjes së individit disponimi për marrjen ose jo në përgjegjësi penale të tij për veprimet e mësipërme duhet të paraprihet nga një trajtim i çështjes nëse shpërndarja e materialit është në përmbushje të lirisë së shprehjes. Për këtë qëllim paraqitet e nevojshme që të vlerësohet nëse rastet objekt i verifikimit të kallëzimit ose hetimit penal përfshihen në kufizimet e parashikuara nga neni 10 i KEDNJ. Në paragrafin e dytë të kësaj dispozite përcaktohen rastet e kufizimit të lirisë së shprehjes të cilat duhet të jenë:

- të parashikuara nga ligji dhe që,
- në një shoqëri demokratike përbëjnë masa të nevojshme,
- në interes të sigurisë kombëtare,
- në interes të integritetit territorial ose sigurisë publike,
- për mbrojtjen e rendit dhe parandalimin e krimit,
- për ruajtjen e shëndetit ose të moralit,
- për mbrojtjen e dinjitetit ose të të drejtave të të tjerëve,
- për të ndaluar përhapjen e të dhënave konfidenciale,
- ose për të garantuar autoritetin dhe paanshmërinë e pushtetit gjyqësor….".[25]

GJEDNJ ka mbajtuar një numër të konsiderueshëm qëndrimesh në të cilat është trajtuar liria e shprehjes në raste të përhapjes së materialeve të lidhura me genocidin. Këto qëndrime edhe pse nuk janë trajtojnë raste të shfrytëzimit të sistemeve kompjuterike, ofrojnë standarte të GJEDNJ tërësisht të aplikueshme edhe për shpërndarjen e materialeve nëpërmjet teknologjisë së informacionit.

Një gjykim i tillë është ai i vitit 1996 Schimanek kundër Austrisë.[26]

23 Shih nenin 12/1 te Kushtetutës së Republikës së Shqipërisë. Botim i "Qendrës së Botimeve Zyrtare". ISBN 978-9928-01-068-1.

24 Në këtë dispozitë parashikohet: "Çdokush ka të drejtën e lirisë së shprehjes. Kjo e drejtë përfshin lirinë e mendimit dhe lirinë për të marrë ose për të dhënë informacione ose ide pa ndërhyrjen e autoriteteve publike dhe pa marrë parasysh kufijtë".

25 Shih nenin 10/2 të Konventës Evropiane të të Drejtave të Njeriut. I disponueshëm në https://www.echr.coe.int/Documents/Convention_ENG.pdf.

26 Çështja Schimanek kundër Austrisë Nr. 32307/96. Information Note on the Court's case-law 15. I disponueshëm në https://hudoc.echr.coe.int/eng?i=002-6091.

Në këtë gjykim aplikanti ishte arrestuar mbi dyshimet se kishte qenë i përfshirë në aktivitete të frymëzuara nga ideologjia Nacional Socialiste. Gjykata e Asizit e dënoi atë mbi bazën e seksionit 3a/2 të Aktit të Ndalimit të Nacional Socializmit dhe e dënoi atë me 15 vjet burgim. U provua se aplikanti, lider i një grupi pro-nazist, kishte qenë i përfshirë në rekrutimin e anëtarëve të rinj dhe kishte organizuar takime ku Rajhu i Tretë ishte glorifikuar dhe ekzistenca e vrasjeve sistematike me anë të gazit toksik në kampet e përqëndrimit ishte mohuar. Gjithashtu ai kishte kontribuuar dhe në shpërndarjen e pamfletave që promovonin këtë ideologji. GJEDNJ ka konstatuar se ndalimi i aktiviteteve lidhur me shprehjen e ideve Nacional Socialiste ishte i parashikuar në ligjin austriak dhe, në këndvështrimin e të kaluarës historike dhe sfondin e Konventës në vetvete, mund të justifikohej se ishte i nevojshëm në një shoqëri demokratike, në interes të sigurisë kombëtare dhe integritetit territorial po ashtu edhe për parandalimin e krimit.[27] Për këto arsye në këtë gjykim nuk është gjetur shkelje e nenit 10 të Konventës.

Në vendimin e mësipërm është trajtuar një rast i miratimit të krimeve kundër njerëzimit, i cili ka arritur në nivelin e glorifikimit të tyre. GJEDNJ duke konstatuar ndalimin e sjelljeve të tilla nga ligji i brendshëm dhe ekzistencën e kushteve të parashikuara për kufizimin e lirisë së shprehjes ka konkluduar se dënimi i aplikantit ka qenë në përputhje me Konventën.

Në një tjetër gjykim është gjetur i papranueshëm nga GJEDNJ aplikimi para asaj gjykate në rastin e dënimit të një shkrimtari, njëherësh filozof dhe politikan, për shkak të kundërshtimit prej tij në një libër të titulluar "Legjendat në rrënjët e politikës izraelite", të krimeve kundër njerëzimit të kryera në dëm të hebrenjve. [28] Në këtë libër aplikanti ka vënë në diskutim vërtetësinë, shkallën dhe gravitetin e fakteve historike të lidhura me Luftën e Dytë Botërore, si persekutimi i hebrenjve nga regjimi nazist, Holokausti dhe gjyqet e Nurembergut. GJEDNJ ka nënvizuar se mohimi i krimeve kundër njerëzimit është një nga format më akute të shpifjes raciale kundrejt hebrenjve dhe një nxitje e urrejtjes për to. Gjithashtu ajo gjykatë ka theksuar se justifikimi i politikave pronaziste nuk mund të gëzojë mbrojtjen e nenit 10 të Konventës dhe mohimi ose rishikimi i fakteve historike të pranuara qartësisht, si Holokausti, janë përjashtuar nga neni 17 i Konventës për t'u mbrojtur nga neni 10 i saj.[29]

27 Po aty.

28 Çështja Garaudy kundër Francës (dec.), no. 65831/01, ECHR 2003-IX. I disponueshëm në https://hudoc.echr.coe.int/eng?i=002-4830.

29 Po aty.

Gjykimi Garaudy kundër Francës ka marrë në shqyrtim një situatë të mohimit të krimeve kundër njerëzimit nëpërmjet parashtrimit të dyshimeve të pabazuara mbi fakte historike të pranuara dhe të provuara gjyqësisht. Ky qëndrim i gjykatës ofron një precedent të rëndësishëm për t'u konsideruar në vlerësimin e fakteve të lidhura më qëndrime mohuese të genocidit dhe krimeve kundër njerëzimit, nëpërmjet sistemeve kompjuterike.

Në të njëjtën frymë më gjykimin Garaudy është edhe një qëndrim i mëparshëm i Komisionit Europian të të Drejtave të Njeriut[30], që ka deklaruar të papranueshëm aplikimin e shtetasit austriak Rebhandl, i cili për shkak të shpërndarjes në një gazetë periodike të përmbajtjeve që përbënin aktivitete Nacional Socialiste[31] ishte dënuar penalisht nga autoritetet austriake të drejtësisë. Në kuadër të procesit gjyqësor të brendshëm mbrojtësi i të pandehurit kishte dorëzuar disa kërkesa për të marrë prova të mëtejshme me qëllim për të provuar që nuk kishin ekzistuar dhoma gazi për vrasjen e hebrenjve nën regjimin nazist. Edhe në këtë rast Komisioni ka arritur në përfundimin se ndërhyrja në të drejtën e lirisë së shprehjes së aplikantit nëpërmjet dënimit penal ishte e parashikuar në ligjin "Akti i Ndalimit të Nacional Socializmit", ka pasur një synim legjitim konkretisht "parandalimin e cënimit të rendit dhe të krimeve" dhe "mbrojtjen e reputacionit ose të të drejtave të të tjerëve". Njëkohësisht ndërhyrja ka qenë e nevojshme në një shoqëri demokratike pasi veprimet e aplikantit, bazuar në nenin 17 të Konventës, nuk gëzojnë mbrojtje nga dispozitat e saj. [32]

Në çështjen Nachtmann kundër Austrisë, aplikanti, një qytetar austriak me banim në Grac, në vitin 1995 u dënua penalisht nga gjykatat autriake, për shkak se u gjet përgjegjës për publikimin e një artikulli në revistën e drejtuar prej tij. Në këtë artikull mohohej dhe minimizohej gjërësisht genocidi i forcave Nacional Socialiste. Në këtë rast gjykata e vendit kishte analizuar detajet e deklaratave ku sugjerohej se numri i viktimave të vrasjeve masive, veçanërisht i hebrenjve, me gaz helmues dhe djegie, ishte tepër i ekzagjeruar dhe teknikisht i pamundur. Komisioni Europian i të Drejtave të Njeriut ka pranuar ndërhyrjen në të drejtën për lirinë e shprehjes sipas nenit 10 të KEDNJ por kjo ndërhyrje është vlerësuar se ka qenë e parashikuar në ligjin e brendshëm, kishte nje qëllim legjitim konkretisht "parandalimin e kaosit dhe krimeve" dhe "mbrojtjen e reputacionit të të tjerëve". Gjithashtu Komisioni është shprehur se ndërhyrja ishte e "nevojshme në një shoqëri

30 Në vijim Komisioni.

31 Aktivitete të tilla ishin të ndaluara në Austri nga "Akti I Ndalimit të Nacional Socializmit".

32 Çështja Rebhandl kundër Austrisë, no. 24398/94, Commission decision of 16 January 1996, unreported. I disponueshëm në https://hudoc.echr.coe.int/eng?i=001-2665.

demokratike" pasi publikimi ka mohuar dhe minimizuar gjërësisht vrasjet masive dhe krime të tjera të kryera nën regjimin Nacional Socialist.[33]

Mohimi apo vënia në dyshim e genocidit apo krimeve kundër njerëzimit mund të shfaqet edhe për disa segmente përbërëse të një fakti penal të provuar ndërkombëtarisht. Një qëndrim i tillë haset në gjykimin me kërkues Hans-Jürgen WITZSCH[34], ku aplikanti, shtetas gjerman, në 3 Dhjetor 1999 i kishte shkruar një historiani të njohur, profesor W, në përgjigje të disa deklaratave të bëra nga ky fundit në shtator 1999 lidhur me qëllimin e Hitlerit për të vrarë hebrenjtë. Në përgjigjen e dhjetorit 1999 aplikanti ishte shprehur ndër të tjera: "Është aktualisht e përcaktuar se nuk ka asnjë indikacion në programin e Partisë Socialiste të Punëtorëve Gjermanë, (NSDAP) që NSDAP dhe Hitleri kishin qëllim të vrisnin hebrenjtë. Shumë kohë më parë, historiani Irving ka propozuar publikisht që të paguante 1000 paund për çdo person që do të mund të provonte që Hitleri kishte urdhëruar, për arsye raciale, vrasjen e një hebreu të vetëm. Deri tani, asnjë nuk ka paraqitur të dhëna. ... Asnjë nga personalitetet e qeverisë gjermane të akuzuar në Nuremberg nuk pranoi të kishte pasur dijeni për vrasjet masive të hebrenjve....". Në 27 Korrik 2001 gjykata deklaroi fajtor aplikantin për denigrimin e dinjitetit të të vdekurve sipas seksionit 189 të Kodit Penal Gjerman dhe e dënoi atë me tre muaj burgim.

GJEDNJ ka trajtuar aplikimin edhe në kuadër të nenit 10 të Konventës. Ajo theksoi se sipas gjykatave gjermane, aplikanti kishte mohuar një fakt historik të pranuar lidhur me përgjegjësinë e Hitlerit dhe të NSDAP në raport me Holokaustin dhe në këto kushte kishte diskretituar dinjitetin e të vdekurve. ... Qëllimi i nenit 17[35] të Konventës është për ta bërë të pamundur për individët për të përfituar nga një e drejtë me synimin për të promovuar ide të kundërta me tekstin dhe frymën e Konventës. Gjykata ka theksuar se aplikanti ka mohuar si Holokaustin si të tillë ashtu edhe ekzistencën e dhomave të gazit. Sidoqoftë, ai mohoi një rrethanë të njëjtë sinjifikative dhe të përcaktuar të Holokaustit duke konsideruar të rreme dhe historikisht të pabazuar që Hitleri dhe NSDAP kishin planifikuar, filluar

33 Çështja Nachtmann kundër Austrisë, no. 36773/97, Commission decision of 9 September 1998, unreported. I disponueshëm në https://hudoc.echr.coe.int/eng?i=001-4399

34 Çështja Witzsch kundër Gjermanisë (nr. 2) (dec.), no. 7485/03, 13 Dhjetor 2005. I disponueshëm në https://hudoc.echr.coe.int/eng?i=001-72786.

35 Ndalimi i abuzimit me të drejtat: "Asnjë nga dispozitat e kësaj Konvente nuk mund të interpretohet se i jep një Shteti, grupimi ose individi, të drejtë që të përfshihet në ndonjë veprimtari ose të kryejë ndonjë akt që synon cënimin e të drejtave dhe lirive të përcaktuara në këtë Konventë ose kufizime më të gjera të këtyre të drejtave ose lirive sesa është parashikuar në Konventë".

dhe organizuar vrasjen masive të hebrenjve. Për këto arsye GJEDNJ ka konkluduar se cënimi i lirisë së shprehjes së aplikantit ka qenë në përputhje me nenin 10/2 të Konventës.

Në gjykimin Perinçek kundër Zvicrës,[36] të lidhur me dënimin penal për refuzimin e karakterizimit ligjor si "genocid" të akteve të kryera nga Perandoria Osmane kundër popullit armen në 1915, Dhoma e Madhe e GJEDNJ gjeti shkelje të së drejtës së lirisë së shprehjes së aplikantit. Në këtë rast Gjykata ka theksuar rëndësinë e analizës së rrethanave të faktit nga gjykatat e brendshme, konkretisht natyrën e deklaratave të bëra, faktorët gjeografikë dhe historikë, faktorin kohë dhe përmasat e ndikimit të deklaratave të kryera.

Në atë gjykim aplikuesi ishte një doktor shkencash juridike dhe kryetar i Partisë së Punëtorëve Turkë në Zvicër. Në vitin 2005 ai mori pjesë në konferenca të ndryshme në të cilat mohoi publikisht që kishte pasur genocid të popullit armen nga Perandoria Osmane në 1915 dhe në vitet në vijim. Në veçanti, ai përshkroi idenë e genocidit armen si nje "gënjeshtër ndërkombëtare". Shoqëria Armeno-Zvicerane dorëzoi një kallëzim penal kundër aplikuesit për shkak të komenteve të tij. Aplikanti u urdhërua të paguajë 100 franga svizerane[37], të pezulluar, një gjobë prej 3000 CHF, të cilat mund të zëvendësoheshin me 30 ditë burgim dhe një shumë prej 1000 CHF në kompensim për shoqatën Armeno-Zvicerane.

Në këtë rast, lidhur me "parandalimin e cënimit të rendit" si pjesë e "synimit legjitim" të kërkuar nga neni 10 i Konventës, Gjykata arriti në përfundimin se nuk kishte prova që ndonjë konfrontim të kishte ndodhur në fakt në të dy tubimet e referuara, në të cilat aplikanti kishte qenë folës dhe të cilat ishin zhvilluar rreth një vit para dënimit të aplikantit. Mbi të gjitha, asnjë nga këto aspekte nuk ishte përmendur nga gjykatat zvicerane në vendimet e tyre në çështjen penale ndaj aplikantit. Për këto arsye ndërhyrja në të drejtën e lirisë së shprehjes së aplikantit nuk kishte ndjekur synimin e "parandalimit të cënimit të rendit".

Lidhur me natyrën e deklaratave të aplikantit Gjykata është shprehur se ato kishin prekur çështje ligjore dhe historike, por në kontekstin në të cilin ishin bërë, në evente publike ku i adresohej mbështetësve të aplikantit, tregon se ai kishte folur si një politikan, jo si një studiues ligjor. Ai kishte marrë pjesë në një debat të shtrirë në kohë që Gjykata e ka pranuar në

36 Perinçek kundër Zvicrës [GC], nr. 27510/08, ECHR 2015 (extracts). Information Note on the Court's case-law 189. I disponueshëm në https://hudoc.echr.coe.int/eng?i=002-10930.

37 CHF.

një numër çështjesh kundër Turqisë, si të lidhur me një çështje me interes publik dhe të përshkruar si "debat të nxehtë, jo vetëm brenda Turqisë por gjithashtu edhe në arenën ndërkombëtare". Gjykata nuk i ka perceptuar këto deklarata si një formë të nxitjes së urrejtjes ose intolerancës. Në këndvështrimin e gjykatës, deklaratat e aplikantit pranohet që kanë qenë të dëmshme dhe reflektonin një pozicion të papajtueshëm të tij por duhet të pranohet se ato duket se përfshijnë një element ekzagjerimi përsa kohë ato synonin të tërhiqnin vëmendjen.

Gjykata ka trajtuar edhe faktorët gjeografikë dhe historikë për të cilët është shprehur se në këndvështrimin e kontekstit historik në shtetet e interesuara, dënimi i Holokaustit edhe kur është veshur si një kërkim historik i paanshëm, pa dyshim tregon një ideologji anti-demokratike dhe anti-Semitike.[38] Sipas Gjykatës nuk është pretenduar se ka pasur një lidhje direkte ndërmjet Zvicrës dhe ngjarjeve që kanë ndodhur në Perandorinë Osmane në 1915 dhe në vitet në vijim. E vetmja lidhje mund të vinte nga prezenca e komunitetit armen në tokën zvicerane por kjo lidhje ishte e parëndësishme. Debati i ndezur nga aplikanti ishte i jashtëm për politikën e Zvicrës, duke konsideruar që ai ishte një i huaj dhe mund të kthehej në vendin e tij. Për më shumë nuk kishte të dhëna që në kohën e deklaratave atmosfera në Zvicër të ishte e tensionuar dhe të mund të rezultonte në thyerje të rëndë ndërmjet turqve dhe armenëve atje. Dënimi penal nuk mund të justifikohet as me situatën në Turqi... madje as gjykatat zvicerane nuk iu referuan kontekstit turk.[39]

Vëmëndje i është kushtuar nga GJEDNJ edhe faktorit kohë për të cilin ajo gjykatë është shprehur se një kohë e konsiderueshme, rreth 90 vjet, kishte kaluar ndërmjet kohës së deklaratave dhe ngjareve tragjike, të cilave ai u ishte referuar dhe në kohën që ai kishte bërë deklaratat, sigurisht kishte shumë pak të mbijetuar nga ngjarjet. Ndërkohë që kjo ishte ende një çështje aktuale për shumë armenë, veçanërisht ato të diasporës, elementi kohë nuk mund të anashkalohet, shprehet gjykata. Ndërsa eventet e një kohe relativisht të afërt mund të jenë aq traumatike sa kërkojnë, për një periudhë kohe, një shkallë të lartë të rregullimit të deklaratave të lidhura me to, nevoja për të tillë rregullim është e destinuar të zbehet me kalimin e kohës. [40]

Sa i takon përmasave të ndikimit të deklaratave Gjykata, në rastin

38 Perinçek kundër Zvicrës [GC], nr. 27510/08, ECHR 2015 (extracts). Information Note on the Court's case-law 189. I disponueshëm në https://hudoc.echr.coe.int/eng?i=002-10930

39 Po aty.

40 Po aty.

Perinçek, ishte e ndërgjegjshme për rëndësinë e pamasë të lidhur me komunitetin armen për çështjen nëse eventet tragjike të vitit 1915 dhe viteve në vijim të shiheshin si genocid dhe ndjeshmërinë akute të komunitetit ndaj çdo deklarate që rëndon në atë pikë. Sidoqoftë, thotë Gjykata, nuk mund të pranohet që deklaratat e aplikuesit të ishin aq të dëmshme për dinjitetin e armenëve që kishin vuajtur e ishin zhdukur në ato evente dhe për dinjitetin dhe identitetin e pasardhësve të tyre sa të kërkonin masa penale në Zvicër. "Pickimi" i deklaratave të aplikantit nuk ishte drejtuar ndaj atyre personave por ndaj "imperialistëve" që ishin parë si përgjegjës për ato mizori. Kjo e parë edhe në raport me kohën që kishte kaluar nga eventet në të cilat aplikanti ishte referuar, e çoi gjykatën në konkluzionin që deklaratat e tij nuk mund të shiheshin sikur kishin pasur efektin sinjifikant shqetësues që nevojitet për legjitimuar kufizimin e lirisë së shprehjes.

Qëndrimet e mësipërme lidhur me faktorët historikë, gjeografikë dhe efektet në shoqëri të deklaratave të kryera, janë konfirmuar nga GJEDNJ edhe në gjykimin Leroy kundër Francës,[41] kur liria e shprehjes është analizuar në kuadër të "krimeve të urrejtjes".[42]

Ashpërsia e dënimit është një tjetër element që duhet të vlerësohet në rastin e analizës së aplikimit të dënimit penal në raport me lirinë e shprehjes. Kështu GJEDNJ në gjykimin Perinçek kundër Zvicrës, konkludoi se nuk kishte qenë e nevojshme në një shoqëri demokratike për të zbatuar ndaj aplikantit një dënim penal në mënyrë që të mbrohen të drejtat e komunitetit armen në diskutim në rastin konkret.[43] Për gjithë arsyet e mësipërme në atë rast është konstatuar shkelje e nenit 10 të KEDNJ.

Proporcionaliteti i ashpërsisë së dënimit për sjelljen e dënueshme, në raport me lirinë e shprehjes është trajtuar nga GJEDNJ edhe në cështjen Dmitriyevskiy kundër Rusisë. Ajo gjykatë është shprehur se duhet të përcaktohet nëse masa e marrë ishte "proporcionale me qëllimin legjitim të synuar". ...Natyra dhe ashpërsia e sanksioneve të vendosura janë faktorë që duhet të merren në konsideratë kur vlerësohet proporcionaliteti i ndërhyrjes në lirinë e shprehjes.[44]

---

41 Çështja Leroy kundër Francës. no. 36109/03, 2 October 2008 I disponueshëm në Leroy v. France (coe.int)

42 Krimet e motivuara nga jo toleranca ndaj grupeve të caktuara në shoqëri përshkruhen si "krime të urrejtjes". Botim I OSBE-ODIHR "Të kuptuarit e krimeve të urrejtjes". I disponueshëm në https://tandis.odihr.pl/bitstream/20.500.12389/21200/8/06995alb.pdf

43 Po aty.

44 Çështja Dmitriyevskiy kundër Rusisë nr. 42168/06, 3 October 2017, I disponueshëm në Dmitriyevskiy v. Russia (coe.int)

Konkluzione

Mos përfshirja në nenin 75/a të Kodit Penal të vendimit gjyqësor ndërkombëtar të formës së prerë mbi kualifikimin e fakteve të shpërndara si genocid apo krime kundër njerëzimit, si parakusht për marrjen në përgjegjësi penale, ka ofruar një mundësi më të gjërë për gjykatat dhe prokuroritë shqiptare. Këto të fundit kanë mundësi për të kualifikuar sipas dispozitës së mësipërme edhe rastet kur janë publikuar materiale të vlerësuara si konsumim i neneve 73 "Genocidi" dhe 74 "Krimet kundër njerëzimit" të K.P. me vendim gjyqësor të formës së prerë të brendshëm. Por vlerësohet se në çdo rast ekzistenca paraprake e një vendimi gjyqësor të formës së prerë, i jashtëm apo i brendshëm, mbi praninë e krimeve të mësipërme është një kusht i domosdoshëm, mungesa e të cilit passjell edhe mungesën e konsumimit të anës objektive të figurës së veprës penale "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit".

Në "Protokollin shtesë", edhe lidhur me dispozitën "Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit", parashikohet se një shtet palë mund të kërkojë që mohimi ose minimizimi i konsiderueshëm i përmendur në paragrafin "1" të këtij neni të jetë kryer për të nxitur urrejtjen, diskriminimin ose dhunën kundër një individi ose grupi individësh, bazuar mbi racën, ngjyrën prejardhjen, origjinën kombëtare ose etnike si dhe fenë, nëse përdoret si pretekst për një nga këta faktorë. Një parashikim i tillë nuk është përthithur në nenin përkatës të Kodit Penal shqiptar, në të cilin penalizohet shpërndarja e materialeve raciste ose ksenofobike edhe kur ato nuk nxisin dhunë apo urrejtje. Vlerësohet se një qëndrim i tillë i ligjvënësit shqiptar, në kushtet kur norma e protokollit ia ka besuar vullnetit të shteteve nënshkruese, është shumë i përshtatshëm pasi garanton një mbrojtje më të gjërë të të drejtave të individit të një përkatësie të caktuar.

Në rastet e shpërndarjes, nëpërmjet sistemit kompjuterik, të materialeve që mbështesin genocidin apo krimet kundër njerëzimit duhet t'i kushtohet rëndësi analizës juridike nëse përhapja e materialeve mbrohet nga liria e shprehjes së individit apo është pjesë e rasteve që justifikojnë kufizimin e kësaj lirie, duke legjitimuar në këtë mënyrë zbatimin e dënimit penal. Për të konkluduar në lidhje me këtë moment është e nevojshme të shqyrtohen disa kritere, konkretisht:

- Duhet kontrolluar nëse dënimi penal është i parashikuar në ligj. Lidhur me këtë komponent është e nevojshme që të përcaktohet propocionaliteti i masës së dënimit me rëndësinë e shkeljes. Në këtë mënyrë sigurohet shmangia e dënimeve të papërshtatshme që do të përbënin cënim të lirisë së

shprehjes së individit.

- Një vëmëndje e veçantë për të konkluduar mbi nevojën e dënimit penal është e lidhur me rrethanat gjeografike dhe historike të faktit objekt hetimi. Këto rrethana duhet të vlerësohen në lidhje me efektin dhe pasojat që mund të shkaktojnë në shoqëri në këndvështrimin e paragrafit të dytë të nenit 10 të Konventës. Vlerësimi i drejtë i rrethanave të mësipërme orienton në arritjen e një rezultati të bazuar mbi faktin nëse dënimi penal është ose jo "i nevojshëm në një shoqëri demokratike".

Bibliografi:

- Konventa mbi Parandalimin dhe Dënimin e Krimit të Genocidit.
- Karta e Gjykatës Ushtarake Ndërkombëtare.
- Konventa Evropiane të të Drejtave të Njeriut.
- Kushtetuta e Republikës së Shqipërisë.
- "Konventa për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
- Ligji nr. 9262, datë 29.7.2004 "Për Ratifikimin e "Protokollit Shtesë të Konventës për Krimin Kibernetik, për Penalizimin e Akteve me Natyrë Raciste dhe Ksenofobe të kryera nëpërmjet Sistemeve Kompjuterike".
- Kodi Penal i Republikës së Shqipërisë.
- "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems".
- Çështja Leroy kundër Francës.
- Çështja Schimanek kundër Austrisë.
- Çështja Garaudy kundër Francës.
- Çështja Rebhandl kundër Austrisë.
- Çështja Nachtmann kundër Austrisë.
- Çështja Witzsch kundër Gjermanisë.
- Çështja Perinçek kundër Zvicrës.
- Çështja Dmitriyevskiy kundër Rusisë.

PËRDORIMI I TEKNOLOGJISË NË PARANDALIMIN E AKTIVITETIT KRIMINAL TË KRIMIT TË ORGANIZUAR BRENDA SISTEMIT PENITENCIAR

PROF.ASOC. DR. SKERDIAN KURTI

Departamenti i së Drejtës Penale

Fakulteti i Drejtësisë, Universiteti Tiranës

skerdian.kurti@fdut.edu.al

Abstrakt

Në bazë të nenit 16 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", Institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë janë institucionet ku ekzekutohen edhe vendimet me burgim për çdo vepër penale të kryer nga pjesëtarët e krimit të organizuar. Ndërkohë sipas nenit 17 të po këtij ligji, në raste të veçanta mund të zbatohet një regjim i posaçëm i ushtrimit të të drejtave për të dënuarit në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë dhe të paraburgosurit që hetohen ose gjykohen për veprat penale të kryera në kuadër të pjesëmarrjes në krim të organizuar.

Qëllimi i këtij punimi është të tregojë se cila është rëndësia e përdorimit të teknologjisë brenda sistemit penitenciar në kuadër të trajtimit të të burgosurve për pjesëmarje në krim të organizuar. Nga ana tjetër, duke ditur që institucionet e ekzekutimit të vendimeve penale shërbejnë jo vetëm për riedukimin e të dënuarve por edhe për parandalimin e kryerjes së veprave penale, sidomos të pjesëtarëve të krimit të organizuar që veprojnë nga brenda institucioneve, do të mundohemi të shpjegojmë rolin që ka teknologjia për realizimin e këtij qëllimi.

Fjalë kyçe: *Krimi i organizuar, Sistemi penitenciar, Teknologjia, Parandalimi, Riedukimi*

1. Hyrje

Sistemi penitenciar është një nga hallkat e rëndësishme të sistemit të drejtësisë penale. Është vendi ku ekzekutohet dënimi me burgim dhe vendosen të paraburgosurit. Nëse nuk do të funksionojë ky sistem nuk do të ketë kuptim asnjë nga rregullat e proçesit të drejtë, pasi nuk do të kishte mundësi të ekzekutohej sipas mënyrës së duhur vendimi penal i formës së prerë. Në këto institucione, nëpërmjet riedukimit të të dënuarve, realizohet ai lloj parandalimi që nga kriminologët njihet me emrin parandalimi i posaçëm i kriminalitetit. Ky lloj parandalimi lidhet me trajtimin e të dënuarve me qëllim që pas vuajtjes së dënimit të jenë të dobishëm për shoqërinë dhe të mos i shkaktojnë dëme asaj.

Personat e dënuar vendosen në institucionet e ekzekutimit të vendimeve penale në bazë të një klasifikimi paraprak[1]. Ky klasifikim bëhet në përputhje me realizimin e funksionit riedukues të dënimit dhe për këtë arsye ndahet në klasifikim të jashtëm dhe klasifikim të brendshëm. Klasifikimi i jashtëm shërben si bazë për të vendosur llojin e institucionit në të cilin personi do të vuajë dënimin: bazohet në kritere objektive të tilla si: mosha, gjinia, lloji i veprës penale, lloji i dënimit, fakti nëse personi është përsëritës ose jo, etj.; ky klasifikim bëhet përpara se personi të vendoset në institucion. Klasifikimi i brendshëm bëhet duke mbajtur parasysh personalitetin, prirjen dhe qëndrimet e personit të dënuar; ky klasifikim bëhet nga institucioni ku do të ekzekutohet dënimi: klasifikimi i brendshëm është rezultat i studimit gjithëplanësh që i bëhet personit të dënuar në fazën e pranimit dhe të materialeve që përmban fashikulli, i cili shoqëron personin.

Sipas nenit 16 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë janë institucionet ku ekzekutohen vendimet me burgim: a) për çdo vepër penale të kryer nga grupi i strukturuar kriminal, organizata kriminale, organizata terroriste dhe banda e armatosur, sipas përcaktimeve të Kodit Penal; b) për veprat penale për të cilat Kodi Penal parashikon dënimin me burgim të përjetshëm; c) për veprat penale të kryera nga përsëritësit, për të cilat gjykata ka dhënë një dënim jo më

1 Shih, V. Hysi, *Penologjia*, Kristalina-KH, Tiranë, 2010, fq. 72.

të vogël se pesëmbëdhjetë vjet burgim; ç) për krimet kundër jetës, për të cilat gjykata ka dhënë një dënim jo më të vogël se njëzet vjet burgim; d) për krimet seksuale me të mitur, sipas përcaktimeve të Kodit Penal. Përveç sa është parashikuar më sipër, në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë ekzekutohet dënimi edhe ndaj të dënuarve të tjerë, të cilët në kryerjen e veprës penale ose gjatë ekzekutimit të dënimit janë karakterizuar nga qëndrime ose sjellje që e bëjnë të pamundur qëndrimin në burgjet e kategorive të tjera[2].

Caktimi fillestar i të dënuarit në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë kryhet nga gjykata që ka dhënë vendimin e dënimit me burgim. Gjithashtu, gjykata e vendit në të cilin ndodhet institucioni i sigurisë së lartë, është kompetente edhe për ndryshimin e sigurisë së të dënuarve, qoftë për ata të dënuar që kalojnë nga siguria e lartë në sigurinë e zakonshme, qoftë për ata të dënuar që kalojnë nga siguria e zakonshme në sigurinë e lartë.

Krimi i organizuar përbën shkallën më të lartë të rrezikshmërisë dhe për këtë arsye lufta ndaj tij kërkon marrjen e masave më të sofistikuara që të mund të japin efektet e dëshiruara. Politika penale shqiptare përsa i përket trajtimit të veprave penale të kryera nga subjekte të krimit të organizuar është e fokuasuar më së shumti në ashpërsimin e dënimit por praktika e vendeve të tjera ka treguar se ashpërsimi i dënimit nuk mjafton për të luftuar këtë fenomen. Për këtë qëllim është e nevojshme të gjendet një mënyrë e përshtatshme dhe specifike për trajtimin e këtyre subjekteve gjatë gjithë periudhës, duke filluar që nga kryerja e hetimeve paraprake dhe deri në përfundim të ekzekutimit të dënimit me burgim. Në përputhje me këtë orientim dhe me qëllimin e luftimit pa ndalesa të krimit të organizuar, legjislatori ynë ka parashikuar ngritjen e një regjimi të posaçëm në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë[3]. Kështu, sipas Ligjit Nr.81/2020 "*Për të drejtat*

2 Shih, S. Kurti, A. Buçpapaj, *Kufizimi i të drejtave të të dënuarve në burgun e sigurisë së lartë*, në Konferencën shkencore ndërkombëtare "*Criminal law between tradition and challenges of actuality*", Fakulteti i Drejtësisë (UT), Onufri, Tiranë, 2017, fq.589. Në të njëjtën mënyrë shprehet edhe Gjykata e Lartë me anë të Vendimt të Kolegjit Penal të Gjykatës së Lartë Nr. 100 datë 10.02.2010. Sipas kësaj jurisprudence, *rrethanat e kryerjes së veprës penale, si dhe rrezikshmëria e autorit, nuk janë një argument i plotë, bindës për vendosjen e të dënuarit në një burg të sigurisë së lartë. Si rrjedhim gjyqtari mund të vendosi në një burg të sigurisë së zakonshme edhe një të dënuar për kryerjen e një vepre penale me rrezikshmëri të lartë shoqërore. Në rast se kërkohet transferimi në një burg të sigurisë së lartë, i takon Gjykatës që, në zbatim të ligjit, mos të shikojë vetëm formën por edhe sjelljen e të denuarit për atë periudhë kohore të vuajtur në burgun e sigurisë së zakonshme*.

3 Trajtimi i personave të privuar nga liria personale që dyshohen ose janë dënuar për shkak se janë pjesë e krimit të organizuar ka qenë objekt i politikave penale të legjislatorit italian. Zbatimi i një regjimi të tillë, të posaçëm, të quajtur "burgu i vështirë" është i parashikuar nga neni 41-*bis*

dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve", parashikohet se, në raste të veçanta mund të zbatohet një regjim i posaçëm i ushtrimit të të drejtave për të dënuarit në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë dhe të paraburgosurit që hetohen ose gjykohen për disa vepra penale të kryera në kuadër të pjesëmarrjes në grup të strukturuar kriminal, organizatë kriminale, bandë të armatosur, organizatë terroriste ose për vepra me qëllime terroriste[4]. Pavarësisht nga sa është parashikuar më sipër, regjimi i posaçëm mund të zbatohet edhe ndaj të burgosurve të cilët kanë rrezikshmëri të lartë për shkak të lidhjeve me pjesëtarët e organizatave kriminale, organizatave terroriste, bandave të armatosura ose të grupeve të strukturuara kriminale.

Bëhet fjalë për një regjim të trajtimit të të burgosurve, që nga njëra anë shërben për të mbrojtur rendin dhe sigurinë publike duke vendosur kontrollin dhe kufizimin e të drejtave të personave me liri të kufizuar pjesëtarë të organizatave kriminale mafioze dhe nga ana tjetër duhet të tregohet kujdes në respektimin e të drejtave të sanksionuara nga dokumentat ndërkombëtarë dhe kryesisht nga Konventa Evropiane për Mbrojtjen e të Drejtave të Njeriut[5].

---

i ligjit italian për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve. *Legge Nr.354 del 26 Luglio 1975 sull'Ordinamento Penitenziario, aggiornato*. Bëhet fjalë për ligjin mbi të drejtat dhe trajtimin e personave të privuar nga liria personale sipas legjislacionit Italian nga i cili është frymëzuar edhe legjislatori ynë për të krijuar regjimin e posaçëm në burgun e sigurisë së lartë.

4 Neni 17, paragrafi 1 i Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*": Në raste të veçanta mund të zbatohet një regjim i posaçëm i ushtrimit të të drejtave për të dënuarit në institucionet e ekzekutimit të vendimeve penale të sigurisë së lartë dhe të paraburgosurit që hetohen ose gjykohen për veprat penale të parashikuara në nenet 79, shkronja "ç", 79/a, 79/b, 230, 230/a, 230/b, 230/c, 230/ç, 231, 232, 232/a, 234, 234/a, 234/b, 265/a, 265/b, 283, paragrafi 3, 283/a, paragrafi 3, 284, paragrafi 3, 284/a, 284/c, paragrafi 3, 284/ç, paragrafi 3, 333, 333/a dhe 334 të Kodit Penal, të kryera në kuadër të pjesëmarrjes në grup të strukturuar kriminal, organizatë kriminale, bandë të armatosur, organizatë terroriste ose për vepra me qëllime terroriste.

5 Disa herë ky regjim ka kaluar në sitën e jurisprudencës së GJEDNJ-së për shkak të ankimeve të shumta që janë bërë kundër këtij regjimi duke e konsideruar torturë apo trajtim ç'njerëzor që bie në kundërshtim me nenin 3 KEDNJ dhe për rrjedhojë duhet të shfuqizohet. Pavarësisht këtyre ankimeve, një numër i madh i vendimeve të Gjykatës së Strasburgut hedhin poshtë paligjshmërinë e këtij regjimi duke sanksionuar domosdoshmërinë dhe përputhshmërinë e tij me parimet e sanksionuara në Konventën Evropiane për të Drejtat e Njeriut. Shih, Vendim i GJEDNJ, datë 8 qershor 1999, Messina vs. Italia; Vendim i GJEDNJ, datë 22 qershor 1999, Rinzivillo vs. Italia; Vendim i GJEDNJ, datë 31 gusht 1999, Di Giovine vs. Italia; Vendim i GJEDNJ, datë 25 nëntor 1999, Marincola vs. Italia; Vendim i GJEDNJ, datë 1 shkurt 2000, Vincenti vs. Italia; Vendim i GJEDNJ, datë 9 janar 2001, Natoli vs. Italia; Vendim i GJEDNJ, datë 28 qershor 2005, Gallico vs. Italia; Vendim i GJEDNJ, datë 10 nëntor 2005, Argenti vs. Italia; Vendim i GJEDNJ, datë 29 qershor 2006, Viola vs. Italia; Vendim i GJEDNJ, datë 11 korrik 2006, Campisi vs. Italia; Vendim i GJEDNJ, datë 15 janar 2008, Bagarella vs. Italia; Venim i GJEDNJ, datë 24 shtator 2015, Paolello vs. Italisë

2. Kufizimi i të drejtave të të burgosurve në regjimin e posaçëm

Siguria e lartë nënkupton një vëmendje më të madhe ndaj të dënuarve që do të vuajnë dënimin në këto institucione: kjo mund të shprehet qoftë nëpërmjet rritjes së sigurisë qoftë nëpërmjet kufizimit të të drejtave. Nevoja për siguruar rendin publik jashtë institucionit por edhe për të shmangur trazirat dhe revoltat brenda në institucion nxisin nevojën për të parandaluar: kontaktet me organizatën kriminale ku bëjnë pjesë apo me organizata të tjera aleate; konfliktet e mundshme me elementë të organizatave kundërshtare; ndërveprimin me të burgosurit apo të paraburgosurit e tjerë që i përkasin të njëjtës organizatë ose të organizatave të tjera me të cilat ata bashkëpunojnë[6]. Sipas legjislacionit tonë, regjimi i posaçëm i ushtrimit të të drejtave konsiston:

- Në lejimin e një takimi në muaj me anëtarë të familjes, i cili kryhet në intervale të rregullta kohore dhe në mjedise të caktuara, ku ndalohet hyrja e personave ose sendeve të tjera dhe që i nënshtrohen regjistrimit audio dhe video. Takimi me persona të ndryshëm nga anëtarët e familjes, për personat e dënuar, lejohet me propozimin e drejtorit të institucionit dhe me miratimin e Drejtorit të Përgjithshëm të Burgjeve. Për personat e paraburgosur, takimi me persona të ndryshëm nga anëtarët e familjes lejohet vetëm me miratimin e prokurorit. Parashikimet e kësaj shkronje nuk zbatohen për takimet me mbrojtësit. Sipas jurisprudencës së GJ.E.D.NJ.-së[7], e cila ka marrë në shqyrtim regjimin e posaçëm italian, kufizimi i takimeve për të burgosurit e vendosur në këtë regjim të parashikuar nga neni 41-bis, legjitimohet nga arsyet e zbatimit të këtij regjimi që synon të shkëpusi lidhjet me mjedisin kriminal të këtyre personave me rrezikshmëri të lartë shoqërore. Sipas jurisprudencës së Gjykatës së Lartë italiane, fëmijës ose nipit me moshë më të vogël se 12 vjeç, i lejohet të kalojë 10 minutat e fundit së bashku me prindin e vendosur në regjimin e posaçëm, me kusht që pjesa tjetër e familjes të jetë larguar nga vendi i takimit dhe i mituri të jetë i shoqëruar nga një polic i burgut në sallën përtej xhamit[8]. Në përputhje me realizimine

6 Sipas jurisprudencës së Gjykatës Kushtetuese italiane, shtrëngimet e vendosura nga administrata penitenciare duhet të jenë të përshtatshme dhe proporcionale, me qëllimin për ruajtjen e sigurisë dhe të rendit publik që është në themel të zbatimit të këtij regjimi, dhe nuk duhet të cënojnë të drejtat që lidhen me nevojat kryesore minimale. Shih, Vendim i Gjykatës Kushtetuese italiane, *C. cost., sent. 14 ottobre 1996, n. 351.*

7 Vendim i GJ.E.D.NJ., datë 25 shtator 2000, sesioni i dytë, Messina vs. Italia.

8 Shih, Vendim i Gjykatës së Lartë italiane, *Cass. Pen. sez. I, 11 giugno 2014, Nr. 39966*, në M. Nestola, *I colloqui ed i detenuti al 41-bis*, në Revistën *Giurisprudenza Penale* (*Revistë on-line*), 2019. Me anë të këtij vendimi, jurisprudence e Gjykatës së Lartë thekson rëndësinë e madhe, në

kësaj të drejte, administrata e institucionit penitenciar Italian është e detyruar të lejojë personin e vendosur në regjimin e posaçëm të ketë takime me përfaqësuesin shpirtëror të fesë që ai praktikon, por ky takim duhet të zhvillohet në mënyrë të tillë që të mos cënohen rendi dhe siguria brenda në institucion[9];

- Në lejimin e të burgosurit për kryerjen e një bisede telefonike në muaj, me kohëzgjatje maksimale dhjetë minuta, e cila regjistrohet. Kryerja e bisedave telefonike për personat e dënuar autorizohet me vendim të arsyetuar të drejtorit të Përgjithshëm të Burgjeve pas propozimit të drejtorit të institucionit, ndërsa për personat e paraburgosur autorizohet me vendim të arsyetuar të prokurorit. Parashikimet e kësaj shkronje nuk zbatohen për kryerjen e bisedave telefonike me institucionin e Avokatit të Popullit dhe me organizata vendase ose të huaja, që veprojnë në fushën e të drejtave të njeriut;
- Në ndalimin e përdorimit të vlerave monetare, sendeve dhe objekteve, që mund të marrë i burgosuri nga jashtë, sipas parashikimeve në rregulloren e brendshme të institucionit. Në lidhje me këtë pikë, referuar jurisprudencës italiane, është konsideruar i ligjshëm dhe në përputhje me Kushtetutën italiane, ndalimi i parashikuar nga legjislatori për të mos lejuar shkëmbimin e librave dhe revistave ndërmjet personave të vendosur në regjimin e parashikuar nga neni 41-bis dhe familjarëve të tyre[10];
- Në kontrollin e korrespondencës, përveç asaj me subjektet e përcaktuara në pikën 1 të nenit 51 DTDBP[11], ose me organizata ndërkombëtare, që

---

kuadër të mbrojtjes së interesit më të lartë të të miturit nën 12 vjeç, që kanë takimet e tyre me prindin dhe sidomos në rastin edhe të kontakteve fizike.

9 Shih, Vendim i Gjykatës së Lartë italiane, Nr.20979, datë 8 mars 2011.

10 Shih, Vendim i Gjykatës Kushtetuese italiane, datë 8 shkurt 2017. Gjithashtu mund të konsultohet edhe komenti mbi këtë vendim: A. Della Bella, *Per la Consulta è legittimo il divieto imposto ai detenuti in 41-bis di scambiare libri e riviste con i familiari,* në *Diritto Penale Contemporaneo (Revistë on-line)*, 2017.

11 Neni 51 paragrafi 1 i Ligjit 81/2020"*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*". Institucionet e ekzekutimit të vendimeve penale mund të vizitohen pa autorizim nga: Presidenti i Republikës, Kryetari i Kuvendit, Kryeministri, kryetari i Gjykatës Kushtetuese, zëvendëskryetari i Kuvendit, zëvendëskryeministri, ministri i Drejtësisë, kryetari i Gjykatës së Lartë, Prokurori i Përgjithshëm, Drejtuesi i Prokurorisë së Posaçme, deputetët, zëvendësministri i Drejtësisë, Avokati i Popullit, komisionerët dhe ndihmëskomisionerët e tij, Komisioneri për Mbrojtjen nga Diskriminimi, drejtori i Përgjithshëm i Burgjeve dhe zëvendësit e tij, drejtori i Policisë së Burgjeve, drejtori dhe inspektorët e kontrollit të brendshëm të burgjeve, anëtarët e komisionit të ekzekutimit të vendimeve penale, gjyqtarët dhe prokurorët gjatë ushtrimit të detyrës së tyre, mbrojtësit e të burgosurve, si dhe oficerët e Policisë Gjyqësore të deleguar.

ushtrojnë veprimtarinë e tyre në fushën e mbrojtjes së të drejtave të njeriut. Sipas jurisprudencës italiane, edhe për të dënuarit e vendosur në regjimin e posaçëm në bazë të nenit 41-bis, kufizimi dhe kontrolli i korrespondencës mund të bëhet vetëm me vendim të motivuar nga ana e gjykatës dhe jo mbi bazën e rregulloreve administrative[12];

- Në uljen e qëndrimit në ajrim në ambiente të hapura deri në 2 orë, por jo më pak se 1 orë në ditë;
- Në përjashtimin nga organet përfaqësuese të të burgosurve.

Sipas jurisprudencës së Gjykatës së Strasburgut, vetëm një izolim total është konsideruar i ndaluar, ndërsa një regjim i tillë i zbatuar për motive të sigurisë që lejon sadopak kontakte me njerëzit dhe me botën e jashtme është legjitim dhe mund të përdoret13. Në një tjetër vendim të saj, ku merr në shqyrtim qëndrimin për periudha të gjata kohe në regjime të posaçme që karakterizohen nga forma izolimi intensive, GJEDNJ ka sanksionuar parimin e përgjithshëm sipas të cilit regjimet e posaçme të kufizimit të lirisë personale në të cilat zbatohen forma të ngjashme me izolimin nuk mund të vendosen për një kohë të pacaktuar për shkak të efekteve të dëmshme që i sjellin shëndetit fizik dhe psikik të të dënuarit[14].

Sipas legjislacionit shqiptar, respektimi i të drejtave të parashikuara në për të burgosurit e vendosur në regjimin e posaçëm monitorohet nga Avokati i Popullit.

3. Përdorimi i teknologjisë në institucionet e ekzekutimit të vendimeve penale

Në ditët e sotme, zhvillimi i teknologjisë ka ndryshuar botën duke shënuar kalimin në një epokë të re kulturore, në një mënyrë të re të menaxhimit të kohës dhë të jetës sociale të gjithë secilit. Këto zhvillime teknologjike, nga njëra anë kanë ndikuar në sofistikimin e sjelljeve kriminale dhe nga ana tjetër kanë

12 Shih, G. Alberti, *In tema di limitazioni del diritto alla corrispondenza per i detenuti sottoposti al regime di cui all'art. 41-bis*, në *Diritto Penale Contemporaneo (Revistë on-line)*, 2016.

13 Shih, Vendim i GJEDNJ, datë 4 shkurt 2003, Van der Ven vs. Holandës, paragrafët 50-51. Vendimi bën fjalë për një regjim që karakterizohet për një kontroll të fortë të të drejtave të njeriut, i ngjashëm me regjimin e parashikuar nga neni 41 bis i legjislacionit italian dhe për të cilin Gjykata e Strasburgut shprehet se është i ligjshëm. Shkelja e nenit 3 K.E.D.NJ. konstatohet vetëm për shkak të disa elementëve të tjerë siç janë kontrollet e shumta trupore.

14 Shih, Vendim i GJEDNJ, datë 18 mars 2014, Ocalan vs. Turqisë. Nga leximi i këtij vendimi arrijmë në konkluzionin se faktori "kohë" merr një rëndësi të veçantë në vlerësimin e përputhshmërisë së këtij regjimi me nenin 3 KEDNJ.

filluar të përdoren edhe nga institucionet përkatëse kompetente me qëllim luftën dhe parandalimin e këtyre sjelljeve kriminale. Gjthçka ka ndryshuar dhe ky ndryshim nuk mund të mos vihej re edhe në mënyrën e menaxhimit të sistemit penitenciar. Trajtimi dhe riedukimi i të dënuarve duket se është bërë më komod nëpërmjet përdorimit të "shpikjeve" teknologjike, të cilat i vijnë në ndihmë jo vetëm të burgosurve por edhe punonjësve që i mbikqyrin dhe që synojnë të realizojnë planin për rehabilitimin e tyre sa më të shpejtë. Duket se zhvillimi i teknologjisë po i ndihmon të gjithë (punonjës dhe të burgosur) të zgjerojnë hapësirat (territoret ku kalon ditën i burgosuri) ku ekzekutohet dënimi me burgim dhe të kenë më shumë kohë në dispozicion: e gjithë kjo shpie në një njohje më të mirë të individit, të personalitetit të tij gjë e cila çon në arritjen e objektivave madhorë ndër të cilat përmendim, ekzekutimin e dënimit penal, riedukimin dhe rehabilitimin e të dënuarit por mbi të gjitha parandalimin e atij lloji të kriminalitetit që mund të kryhet nga një kategori e caktuar personash, që kanë qënë të përfshirë më parë në sjellje kriminale.

Një nga të drejtat më të rëndësishme për të burgosurit është e drejta për të zhvilluar takime dhe vizita, për të mbajtur korrespondenca dhe për t'u informuar, një e drejtë kjo e ndikuar më së shumti nga zhvillimet teknologjike. Sipas një ndër parimeve themelore që karakterizojnë Rregullat Evropiane të Burgjeve, jeta në burg duhet të përafrohet sa më shumë të jetë e mundur me aspektet pozitive të jetës në një shoqëri të lirë. Mungesa e përdorimit të teknologjisë, e imponuar në burgje, e bën jetën brenda sistemit penitenciar jashtëzakonisht të ndryshme nga jeta jashtë këtij sistemi, duke krijuar një hendek të thellë izolimi të mëtejshëm. Sipas mendimit tonë, "analfabetizmi kompjuterik" heq çdo shtysë të shëndetshme për riintegrim social të të burgosurve. Sipas nenit 24 të Rregullave Evropiane të Burgjeve, të burgosurit duhet të lejohen të komunikojnë sa më shpesh të jetë e mundur nëpërmjet letrave, telefonit ose mjeteve të tjera të komunikimit me familjen, me palët e treta dhe me përfaqësues të organeve të ndryshme, dhe të marrin vizita nga persona të tillë. Në interpretim të këtij neni, mund të themi se autoritetet e burgjeve duhet të jenë të vetëdijshme për mundësitë e reja të komunikimit elektronik që ofron teknologjia moderne. Sa më shumë të zhvillohen këto mundësi, aq më shumë rriten mjetet për kontrollin e tyre, në mënyrë që mjetet e reja të komunikimit elektronik të përdoren në mënyra që nuk kërcënojnë sigurinë dhe rendin e brendshëm. Rregullat "*Mandela Rules*" të Kombeve të Bashkuara, në nenin 58 sanksionojnë se komunikimi me familjen dhe miqtë duhet të bëhet me shkrim dhe duke përdorur, aty ku është e mundur, mjete të telekomunikacionit, elektronik, dixhital apo dhe

mjete të tjera. Një parim i tillë, që e nështron mundësinë e komunikimit elektronik me disponibilitetin e teknologjive të përshtatshme shpjegohet nga konteksti global të cilit i drejtohen Rregullat e Mandelës, ku sigurisht që një vend si Shqipëria gjen vështirësi të mëdha në këtë drejtim.

Ligji i brendshëm shqiptar nuk përcakton shprehimisht të drejtën e të burgosurve për të përdorur teknologjitë e reja të komunikimit. Megjithatë, në paragrafin e shtatë të nenit 49 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", sanksionohet se personeli i institucionit vë në dispozicion të të burgosurit mjetet e nevojshme për realizimin e korrespondencës. Për të burgosurit që nuk kanë mundësi financiare, personeli i institucionit mundëson kartë me impulse ose siguron takime *online* nga institucioni. Ndërsa sipas paragrafit të dhjetë të po këtij neni thuhet se të burgosurit lejohen të mbajnë gazeta, revista e libra, që janë në shitje të lirë dhe të shfrytëzojnë mjete të tjera informacioni. Në interpretim të këtyre dispozitave, ne jemi të mendimit se përdorimi i teknologjisë për realizimin e kësaj të drejte në sistemin penitenciar shqiptar është e lejuar dhe e mbështetur plotësisht në ligj por duhet të përcaktohet më në detaje mënyra e përdorimit të këtyre mjeteve me qëllim që nga njëra anë të burgosurit të mund të komunikojnë me familjen dhe me miqtë e tyre dhe nga ana tjetër përdorimi i teknologjisë të mos shkaktojë cënim të rendit dhe sigurisë në institucion. Sipas paragrafit të katërmbëdhjetë të nenit 49 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", rregulla të detajuara, për kryerjen e vizitave, takimeve dhe mbajtjes së korrespondencës përcaktohen në rregulloren e përgjithshme të burgjeve.

Sipas mendimit tonë, një mënyrë komunikimi e lejueshme dhe e përdorshme mund të jetë edhe komunikimi nëpërmjet skype, në të gjitha ato institucione të ekzekutimit të vendimeve penale që janë të pajisura me kompjuter.

Në përputhje me këtë arsyetim, ne jemi të mendimit se përdorimi i teknologjisë duhet të përfshijë edhe miratimin e kartelës mjekësore dixhitale, thelbësore për të siguruar vazhdimësinë terapeutike, për të monitoruar gjendjen e të burgosurve dhe duke promovuar në këtë mënyrë telemjekësinë. Në ditët e sotme, asnjë institucion penitenciar shqiptar nuk është i pajisur me kartelë mjekësore dixhitale. Gjithçka regjistrohet në dosje letre që datojnë që në kohët më të hershme të krijimit të sistemit penitenciar dhe realizimit të të drejtës për përkujdesje shëndetësore: dosje të mëdha plot me shumë fletë, të dëmtuara, të shkruara me dorë dhe shpesh të pakuptueshme, me rrezikun për të mos jenë në gjendje të japin indikacionet e duhura terapeutike në

situata kritike dhe duke kompromentuar fuqishëm të drejtën për përkujdesje shëndetësore.

Domosdoshmëria e përdorimit të teknologjisë, edhe në sistemin penitenciar, është rritur ndjeshëm pas pandemisë së shkaktuar nga Covid-19. Kjo përfshin jo vetëm zhvillimin e jetës brenda institucionit të ekzekutimit të vendimeve penale por edhe mënyrën e zhvillimit të proceseve gjyqësore penale. Kujtojmë që në sistemin penitenciar qëndrojnë edhe të paraburgosur të cilët janë në proces hetimi apo edhe gjykimi në lidhje me akuzat e ngritura ndaj tyre dhe nga ana tjetër nuk duhet të harrojmë se të gjithë të burgosurit kanë të drejtë të paraqesin kërkesa në gjykatë në lidhje rivendosjen e të drejtave të cënuara gjatë procesit të ekzekutimit të vendimit penal. Sipas mendimit tonë, pjesa teorike nuk duhet të shikohet e ndarë nga pjesa praktike dhe për këtë qëllim, ndoshta, gjëja më e jashtëzakonshme që duhet të ndodhë tani për ata që njohin botën e burgjeve është lejimi i përdorimit të *smartfonëve*: një nga objektet më të demonizuara nga sistemi i burgjeve duhet që të blihet nga vetë institucioni dhe të vihet në shërbim të të burgosurve.

Një e drejtë tjetër e rëndësishme që mund të realizohet nëpërmjet përdorimit të teknologjisë është e drejta për arsim. Sipas nenit 45 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", arsimimi dhe formimi kulturor e profesional bëhen me anë të organizimit të programeve arsimore, si dhe të kurseve profesionale, sipas legjislacionit në fuqi për sistemin arsimor parauniversitar dhe legjislacionit në fuqi për arsimin dhe formimin profesional. Të burgosurit që nuk ka përfunduar arsimin nëntëvjeçar i krijohen kushte për përfundimin e tij me anë të një programi të veçantë, të miratuar nga ministria përgjegjëse për arsimin. I burgosuri ka të drejtë të vazhdojë arsimin e mesëm dhe të lartë gjatë kohës së qëndrimit në institucion, sipas rregullave të parashikuara në legjislacionit për arsimin parauniversitar dhe arsimin e lartë dhe kërkimin shkencor në institucionet e arsimit të lartë. Në interpretim të këtyre dispozitave ligjore, ne jemi të mendimit se një mënyrë për realizimin e të drejtës për arsim lidhet me faktin se institucionet penitenciare duhet të lejojnë mbajtjen e provimeve të diplomës, provimeve universitare dhe intervistave didaktike mes profesorve dhe studentëve në burg, nëpërmjet përdorimit të videokonferencës dhe/ose nëpërmjet *skype*. Gjithashtu, për të kufizuar shqetësimin e të burgosurve që duan të studiojnë, veçanërisht nëse janë të regjistruar në kurse universitare, duhet të lejohet përdorimi i postës elektronike edhe për komunikim të shpejtë me profesorët.

Përdorimi i kamerave në mjediset e brendshme të institucioneve penitenciare ka një rëndësi jo vetëm përsa i përket ruajtjes së rendit dhe

sigurisë në institucion por edhe për të mbikqyrur të burgosurin në rastin e zbatimit ndaj tij qoftë të masave disiplinore qoftë përsa i përket regjimit të mbikqyrjes së veçantë. Në rastin e zbatimit të masave disiplinore të përjashtimit nga veprimtari të përbashkëta apo ajrosja në grup, i burgosuri vendoset në dhomat e veçimit për periudhën e kohës së zgjatjes së masës disiplinore dhe, sipas mendimit tonë, një rëndësi të madhe në vëzhgimin e të burgosurit gjatë kësaj kohe merr edhe përdorimi i kamerave të vendosura në këto ambiente. Me rëndësi më të madhe, ne e shikojmë përdorimin e kamerave në zbatimin e regjimit të mbikqyrjes së veçantë. Sipas nenit 68 të Ligjit Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*", i burgosuri mund të vendoset nën regjimin e mbikëqyrjes së veçantë për një periudhë jo më të gjatë se 3 muaj kur: a) rrezikon sigurinë e personelit të institucionit, vizitorëve, ose kur ka rrezik të dëmtojë veten ose të tjerët; b) ka rrezik të pengojë veprimtarinë e të burgosurve të tjerë nëpërmjet dhunës ose kërcënimeve; c) ka rrezik të detyrojë të burgosurit e tjerë që t'iu nënshtrohen ose të përfitojë prej tyre; ç) pengon të burgosurit e tjerë të mos zbatojnë rregullat individualisht ose në grup ose nxit shkeljen e tyre. Regjimi i mbikëqyrjes së veçantë zbatohet në mjediset e brendshme të institucionit ku ndodhet i burgosuri. Në interpretim të këtyre dispozitave, mund të themi se kemi të bëjmë m një regjim të ndryshëm nga masat disiplinore apo edhe nga regjimi i posaçëm në institucionin e sigurisë së lartë. Në rastin e regjimit të mbikqyrjes së veçantë, i burgosuri qëndron në mjediset ku ai qëndron zakonisht por ndaj tij zbatohet një vëzhgim i veçantë gjatë gjithë kohës për të parë lëvizjet dhe sjelljen e tij në institucion. Pikërisht për të realizuar këtë objektiv, përdorimi i kamerave është opsioni më i mirë i mundshëm por, sigurisht, në përputhje edhe me parimet e sanksionuara nga Gjykata Evropiane e të Drejtave të Njeriut përsa i përket ruajtjes së privatësisë së të dënuarve.

4. Teknologjia dhe regjimi i posaçëm në institucionin e sigurisë së lartë

Në regjimin e posaçëm në institucionin e sigurisë së lartë mund të përdoren dhe të përfitohet nga të mirat që sjellin zhvillimet teknologjike por brenda kufijve të caktuar për shkak të realizimit të qëllimit të zbatimit të këtij regjimi që është ruajtja e rendit dhe e sigurisë publike duke mos lejuar anëtarët e krimit të organizuar që të kenë kontakte me organizatat kriminale që u përkasin apo me të cilat bashkëpunojnë për realizimin e aktiviteteve kriminale. Nisur nga ky arsyetim, mund të themi se përdorimi i teknologjisë

në regjimin e posaçëm nuk mund të jetë në të njëjtin nivel me përdorimin e teknologjisë në regjimet e tjera të sistemit penitenciar. Disa nga rastet kur mund të përdoret teknologjia dhe që përmban edhe rekomandimet e Komitetit për Parandalimin e Torturës (KPT): *Përdorimi i video-konferencave*. KPT rekomandon që zgjatja e regjimit të posaçëm të bazohet në një vlerësim individual të rrezikut që ofron arsye objektive për vazhdimin e masës dhe jo thjesht mungesën e informacionit për të treguar se personi në fjalë nuk është më i lidhur me një organizatë të veçantë. Sa herë që një i burgosur i nënshtrohet rinovimit ose vendosjes për herë të parë të regjimit të posaçëm, atij duhet t'i jepet mundësia të dëgjohet personalisht nga autoriteti ministror kompetent, mundësisht përmes një sistemi me video-konference; *Mbikqyrja me kamera*. KPT ka shprehur shpesh herë shqetësime serioze për faktin se të burgosurit e regjimit të posaçëm i nënshtrohen mbikëqyrjes sistematike dhe të përhershme me kamera brenda qelive të tyre. Një praktikë e tillë sistematike duket të jetë joproporcionale dhe cenon rëndë privatësinë e të burgosurve dhe gjithashtu e bën të gjithë regjimin edhe më shtypës, veçanërisht nëse zbatohet për periudha të gjata. KPT pranon se mbikëqyrja me kamera brenda qelive mund të justifikohet në raste individuale, për shembull kur një person konsiderohet të jetë në rrezik të vetë-lëndimit ose vetëvrasjes ose nëse ekziston një dyshim konkret se një i burgosur po kryen aktivitete në qeli që mund të rrezikojnë sigurinë. Vendimi për të vendosur mbikqyrje me kamera ndaj një të burgosuri të caktuar duhet të bazohet gjithmonë në një vlerësim individual të rrezikut dhe duhet të rishikohet rregullisht. Duhet të ndërmerren hapa për t'u siguruar që të burgosurve që i nënshtrohen mbikëqyrjes me kamera u garantohet një privatësi e arsyeshme kur përdorin tualetin, lavamanin dhe dushin përmes, për shembull, mbulimit të zonës së tualetit në ekranin e monitorit të kamerave.

Sipas mendimit tonë, përdorimi i teknologjisë në regjimin e posaçëm është i rëndësishëm me qëllim parandalimi, kontrollin dhe asgjësimin e sendeve të ndaluara që të burgosurit e këtij regjimi mundohen të mbajnë për të mos humbur kontaktet me botën e jashtme të krimit të organizuar. Në ditët e sotme, instrumentet e komunikimit kanë përmasa gjithnjë e më shumë të vogla saqë mund të fshihen kudo, qoftë në dhomat e të burgosurve qoftë në pjesë të ndryshme të trupit duke e bërë tepër të vështirë zbulimin e tyre me anë të pajisjeve që janë aktualisht në institucionet penitenciare; por jo vetëm kaq, këto instrumente komunikimi mund të transportohen kudo edhe nga një institucion në tjetrin gjatë transferimit të të burgosurve. Kësaj i shtohen edhe instrumentet e komunikimit të kamufluara saqë ngjajnë si sende të lejuara, p.sh., orë dore, stilolaps etj. Për këtë arsye, duhet të

përdoren instrumenta të teknologjisë së avancuar të cilët bëjnë të mundur zbulimin dhe eliminimin e sendeve që mund të indihmojnë të burgosurit e këtij regjimi për të mbajtur kontakte me botën e jashtme të krimit. Një ide është krijimi i një salle qëndrore ndërveprimi dhe një *web application* që ka kontroll mbi të gjitha nivelet e sigurisë dhe që është në gjendje të kontrollojë të gjitha telekamerat e instaluara në institucion. Një sugjerim tjetër është krijimi i një zbuluesi kalimi me sensor të dyfishtë dhe i aftë që të dallojë për çdo pjesë të trupit praninë e objekteve që nuk lejohen. Krahas këtij mund të instalohet edhe një zbulues më rreze X. Një ide tjetër është përdorimi i një sistemi të individualizimit të frekuencave që lejon të kapi të gjitha frekuencat që janë sot në përdorim përfshirë WiFi dhe Bluetooth dhe që është lehtësisht i lëvizshëm nga përdoruesi.

Të gjitha këto ndërhyrje për ta bërë më të fortë regjimin e posaçëm kërkojnë edhe mbrojtje penale, duke shtuar në Kodin Penal edhe një nen që të ndëshkojë të gjithë ata që lejojnë të burgosurit e këtij regjimi të komunikojnë me të tjerët jashtë kushteve të përcaktuara nga legjislacioni në fuqi.

5. Konkluzione dhe rekomandime

Përdorimi i tekonologjisë në kuadër të parandalimit dhe luftës së kriminalitetit përbën një strategji të mirëfilltë që përcakton objektivat për rritjen dhe zhvillimin e çdo vendi dhe që para së gjithash kërkon përdorimin më të mirë të potencialit të teknologjive të informacionit dhe komunikimit për të nxitur inovacionin, rritjen ekonomike dhe përparimin. Personat e burgosur apo janë ndër kategoritë më pak të favorizuara përballë zhvillimeve të njëpasnjëshme të teknologjisë, dhe kjo në mungesë edhe të programeve të ndërhyrjes, të jashtëzakonshme dhe urgjente, që synojnë përshtatjen e trajtimit në institucion dhe rregullsinë e ekzekutimit të vendimit penal me zhvillimin e teknologjisë së informacionit.

Krimi i organizuar, më së shumti, e shfrytëzon zhvillimin e teknologjisë për të realizuar qëllimet e veta, kryerjen e aktiviteteve kriminale dhe pastrimin e parave që vijnë si pasojë e këtyre aktiviteteve kriminale dhe kjo ndodh edhe nga qelia ku anëtarët e këtij lloji të kriminalitetit janë duke vuajtur dënimin. Për këtë arsye është e domosdoshme që edhe në institucionet penitenciare të përdoren të mirat e zhvillimeve teknologjike me qëllim neutralizimin e këtyre përpjekjeve për të kryer aktivitet kriminal nga brenda qelisë së vuajtjes së dënimit. Sipas mendimit tonë, në regjimin e posaçëm në institucionin e sigurisë së lartë, në mënyrë të veçantë duhet të merren masa për të parandaluar dhe asgjësuar futjen e aparateve të jashtëligjshëm që nuk lejohen të futen

brenda institucionit dhe që mund të shërbejnë për të transmetuar mesazhe të shkruajtur apo mesazhe zanore apo edhe objekte metalike që mund të cenojnë rendin dhe sigurinë brenda në institucion. Përveç masave të reja parandaluese duhet të nxitet përdorimi i aparaturave zbuluese që gjenden në institucion me qëllim vëzhgimin konstant të të burgosurve në regjimin e posaçëm por edhe i aparaturave që janë krijuar si pasojë e zhvillimeve teknologjike dhe që ndihmojnë për arritjen e këtyre objektivave. Duhet të shtohen aktivitetet e kontrollit për sende të palejuara, të fshehura në pjesë të ndryshme të trupit apo edhe në dhomën e qëndrimit të cilat në shumë raste nuk mund të dallohen lehtësisht nga punonjësit e shërbimit dhe që mund të sinjalizohen nga aparaturat e sipër përmendura.

Përveç, sa përmendëm më sipër, ne jemi të mendimit që duhet ndërhyrë në Kodin Penal duke ndëshkuar të gjitha ato sjellje të jashtëligjshme që lejojnë apo ndihmojnë të burgosurin që gjendet në regjimin e posaçëm të komunikojë jashtë rasteve të lejuara nga parashikimet ligjore.

Bibliografia

Alberti G., *In tema di limitazioni del diritto alla corrispondenza per i detenuti sottoposti al regime di cui all'art. 41-bis*, në Diritto Penale Contemporaneo (Revistë on-line), 2016.

Della Bella A., *Per la Consulta è legittimo il divieto imposto ai detenuti in 41-bis di scambiare libri e riviste con i familiari***,** në Diritto Penale Contemporaneo (Revistë on-line), 2017.

Hysi V., *Penologjia*, Kristalina-KH, Tiranë, 2015.

Kurti S., Buçpapaj A., *Kufizimi i të drejtave të të dënuarve në burgun e sigurisë së lartë*, në Konferencën shkencore ndërkombëtare "*Criminal law between tradition and challenges of actuality*", Fakulteti i Drejtësisë (UT), Onufri, Tiranë, 2017.

Nestola M., *I colloqui ed i detenuti al 41-bis*, në Revistën Giurisprudenza Penale (revistë on-linë), 2019

Vendim i GJEDNJ, datë 8 qershor 1999, Messina vs. Italia; Vendim i GJEDNJ, datë 22 qershor 1999, Rinzivillo vs. Italia; Vendim i GJEDNJ, datë 31 gusht 1999, Di Giovine vs. Italia; Vendim i GJEDNJ, datë 25 nëntor 1999, Marincola vs. Italia; Vendim i GJEDNJ, datë 1 shkurt 2000, Vincenti vs. Italia; Vendim i GJEDNJ, datë 9 janar 2001, Natoli vs. Italia; Vendim i GJEDNJ, datë 28 qershor 2005, Gallico vs. Italia;

Vendim i GJEDNJ, datë 10 nëntor 2005, Argenti vs. Italia; Vendim i GJEDNJ, datë 29 qershor 2006, Viola vs. Italia; Vendim i GJEDNJ, datë 11 korrik 2006, Campisi vs. Italia; Vendim i GJEDNJ, datë 15 janar 2008, Bagarella vs. Italia; Venim i GJEDNJ, datë 24 shtator 2015, Paolello vs. Italisë; Vendim i GJEDNJ, datë 4 shkurt 2003, Van der Ven vs. Holandës; Vendim i GJEDNJ, datë 18 mars 2014, Ocalan vs. Turqisë.

Vendim i Gjykatës Kushtetuese italiane, datë 14 ottobre 1996; Vendim i Gjykatës Kushtetuese italiane, datë 8 shkurt 2017; Vendim i Gjykatës së Lartë italiane, datë 11 giugno 2014, Nr. 39966; Vendim i Gjykatës së Lartë italiane, Nr.20979, datë 8 mars 2011.

Legge Nr.354 del 26 Luglio 1975 *sull'Ordinamento Penitenziario*, aggiornato.

Ligji Nr.81/2020 "*Për të drejtat dhe trajtimin e të dënuarve me burgim dhe të paraburgosurve*"

KRIMI KIBERNETIK DHE SIGURIA KIBERNETIKE

DR. ELA KERKA

ela.podgorica@fdut.edu.al

MSC. SONJA MEMOÇI

sonjamemoci2@gmail.com

Abstrakt

Krimi kibernetik vazhdon të zgjerohet në shtrirje dhe ndikim. Ekonomitë dhe shoqëritë dixhitale janë një objektiv tërheqës për kriminelët kibernetikë. Inovacioni teknologjik ka perspektiva te mëdha për bizneset dhe qytetarët, por gjithashtu krijon vektorë të rinj sulmi për ata kriminelë që kërkojnë të përfitojnë nga këto zhvillime. Rritja e lidhjes së internetit me qytetarët, bizneset dhe sektori publik, së bashku me rritjen eksponenciale të numrit të pajisjeve dhe sensorëve të lidhur si pjesë e Internetit, po krijon mundësi të reja për kriminelët kibernetikë. Shqipëria është kategorizuar si një vend ku zhvillimi i teknologjisë, aksesi në internet dhe procesi i informimit kanë bërë një progres të shpejtë. Rritja e përdorimit të komunikimit është një vlerë e shtuar në zhvillimin social të vendit, por në të njëjtën kohë e ekspozon vendin ndaj rrezikut të natyrës kibernetike me aktorë qeveritarë apo joqeveritar. Për parandalimin dhe luftimin e krimit kibernetik, Shqipëria ka ratifikuar "Konventën e Budapestit për krimin kibernetik" si dhe ka përfshirë në Kodin Penal disa akte penale kibernetike, me ligjin nr.10023, datë 27.11.2008 dhe disa shtesa të tjera në ligj. nr.7895, datë 27.01.1995 "Kodi Penal i Republikës së Shqipërisë", në kuadër të harmonizimit të legjislacionit të brendshëm me acqius-communitaries veçanërisht me parashikimet e konventës. Qëllimi i punimit është pikërisht studimi i fenomenit të krimit kibernetik, duke analizuar dispozitat ligjore në kuadër të përcaktimeve dhe përmbajtjes së

"Konventës së Budapestit për krimin kibernetik".

Fjalët kyçe: krim kibernetik, kod penal, teknologji, harmonizim, kompjuter

Informacion biografik për autorin prezantues:

Sonja Memoçi, asistent avokate, ka përfunduar studimet Bachelor në Fakultetin e Drejtësisë, Universiteti i Tiranës në vitet 2016-2019. Në vitin 2019-2021 vazhdoi studimet Master Shkencor në të Drejtën Penale. Të dy ciklet e studimeve Bachelor dhe Master kanë përfunduar me rezultate të larta. Gjatë viteve 2019-2020, znj. Memoçi ka punuar si juriste pranë shoqërisë ZICO SH.A. Aktualisht ajo është duke ndjekur studimet në Shkollën e Avokatisë.

Hyrje

Krimi kibernetik është çdo aktivitet kriminal që përfshin një kompjuter, pajisje në rrjet ose një rrjet.

Ndërsa shumica e krimeve kibernetike kryhen me qëllim që të gjenerojnë fitime për kriminelët kibernetikë, disa krime kibernetike kryhen kundër kompjuterave ose pajisjeve drejtpërdrejt për t'i dëmtuar ose çaktivizuar ato. Të tjerë përdorin kompjutera ose rrjete për të përhapur malware, informacione të paligjshme, imazhe ose materiale të tjera. Disa krime kibernetike i bëjnë të dyja -- d.m.th., synojnë kompjuterët për t'i infektuar ata me një virus kompjuterik, i cili më pas përhapet në makina të tjera dhe, ndonjëherë, në rrjete të tëra.

Një efekt primar i krimit kibernetik është financiar. Krimi kibernetik mund të përfshijë shumë lloje të ndryshme të veprimtarisë kriminale të drejtuar nga fitimi, duke përfshirë sulmet e ransomware, mashtrimin me email dhe internetin, dhe mashtrimin e identitetit, si dhe përpjekjet për të vjedhur llogaritë financiare, kartat e kreditit ose informacione të tjera të kartave të pagesave.

Kriminelët kibernetikë mund të synojnë informacionin privat të një individi ose të dhënat e korporatës për vjedhje dhe rishitje. Ndërsa shumë punëtorë vendosen në rutinat e punës në distancë për shkak të pandemisë,

krimet kibernetike pritet u rritën në frekuencë në vitin 2021, duke e bërë veçanërisht të rëndësishme mbrojtjen e të dhënave 'back-up'[1].

Domosdoshmëria e lidhjes me internet ka mundësuar një rritje të vëllimit dhe ritmit të aktiviteteve të krimit kibernetik sepse krimineli nuk ka më nevojë të jetë fizikisht i pranishëm në kryerjen e një krimi. Shpejtësia, komoditeti, anonimiteti dhe mungesa e kufijve të internetit i bëjnë variacionet e bazuara në kompjuter të krimeve financiare -- të tilla si ransomware, mashtrimi dhe pastrimi i parave, si dhe krime të tilla si ndjekja dhe ngacmimi -- më të lehta për t'u kryer.

Veprimtaria kriminale kibernetike mund të kryhet nga individë ose grupe me aftësi relativisht të vogla teknike, ose nga grupe kriminale globale shumë të organizuara që mund të përfshijnë zhvillues të aftë dhe të tjerë me ekspertizë përkatëse. Për të reduktuar më tej shanset e zbulimit dhe ndjekjes penale, kriminelët kibernetikë shpesh zgjedhin të operojnë në vende me ligje të dobëta ose inekzistente për krimin kibernetik.

1. Sfidat dhe e ardhmja e sigurisë kibernetike

Krimi kibernetik është kthyer në sfidë për shoqërinë e sotme. Përdorimi i teknologjive të reja të informacionit dhe veçanërisht i Internetit ka marrë një rëndësi të veçantë në jetën e përditshme. Ky fenomen prek jo vetëm aktivitetet e një organizmi qoftë ai shtetëror apo privat, i implikuar në sferën e biznesit apo të një aktiviteti jo fitimprurës, por mund te prekë dhe njeriun e thjeshtë në aktivitetin e tij të përditshëm, në sferën e tij private apo profesionale. Si çdo teknologji e re e vënë në dispozicion të një numri të madh përdoruesish, Interneti paraqet jo vetëm të mira dhe përfitime, por në të njëjtën kohë dhe një sërë problemesh.

Në vitet e fundit, shoqëritë në të gjithë botën kanë bërë përparime të mëdha drejt kalimit në një shoqëri të informacionit. Teknologjia e informacionit dhe komunikimit tani përshkon pothuajse çdo aspekt të jetës së njerëzve. Fakti që shoqëria po mbështetet gjithmonë e më shumë, e si rrjedhojë, po varet gjithmonë e më shumë nga teknologjia e informacionit dhe komunikimit e bën atë të ekspozuar ndaj kërcënimeve të tilla si krimi kibernetik, domethënë krimi i kryer kundër të dhënave dhe sistemeve kompjuterike ose nëpërmjet tyre. Përveç një numri të madh veprash penale kundër teknologjisë së informacionit dhe komunikimit ose nëpërmjet saj, një numër gjithmonë e më i lartë i çështjeve të tjera që përfundojnë në gjykatë përfshijnë provat

1 techtarget.com/searchsecurity/definition/cybercrime

elektronike që janë memorizuar në një sistem kompjuterik ose në pajisje të tjera.

Derisa teknologjia po arrin të ketë një rol të madh në jetën tonë të përditshme, në anën tjetër, krimi kibernetikë po vazhdon të rritet së bashku më përparimet teknologjike. Krimi kibernetik është një term i cili përdoret për çdo aktivitet të paligjshëm që mundësohet duke përdorur kompjuterët si mjet kryesor për kryerje të veprës.[2] Sipas Strategjisë të Sigurisë Kibernetike të Bashkimit Evropian, "kriminaliteti kibernetik i referohet përgjithësisht një spektri të gjerë veprimtarish kriminale të ndryshme, ku kompjuterët dhe sistemet informative angazhohen ose si vegël primare ose si shënjestër primare. Krimi kibernetik përfshin veprat penale tradicionale (p.sh. mashtrimi, falsifikimi dhe thyerja e identitetit), veprat në lidhje me përmbajtjen (p.sh. shpërndarja në Internet e pornografisë së fëmijëve apo nxitja e urrejtjes racore), si dhe veprat që janë unike për kompjuterë dhe sisteme informative (p.sh. sulmet ndaj sistemeve informative, mohimi i shërbimit dhe malëare."

Kërcënimet kibernetike, tanime janë bërë serioze dhe destabilizuese dhe vazhdimisht janë në rritje. Sipas një studimi të teknologjisë amerikane është e zbuluar se kompanitë besojnë se sulmet kibernetike janë një kërcënim serioz për të dhënat e tyre dhe vazhdimësinë e biznesit të tyre. Sipas të njëjtit studim, vetëm një e treta e kompanive janë plotësisht të sigurt sa i përket sigurisë së informacionit të tyre, madje janë edhe më pak të sigurt kur bëhet fjalë për masat e sigurisë të partnerëve të tyre të biznesit[3].

2. Statistikat e krimit kibernetik ne Shqiperi dhe si ka ndikuar pandemia Covid 19

Pandemia e COVID -19 ka shtuar përdoruesit e internetit dhe ka lulëzuar tregtinë online, duke krijuar terren të favorshëm për sulmet kibernetike. Një situatë që kërcënon të gjithë ata që navigojnë në rrjet dhe që me hapin e kohës, po përpiqen të përshtaten me teknologjinë.

Krimi kibernetik është një fenomen në rritje në Shqipëri. Viti 2021 edhe për shkak të pandemisë ka shënuar rritje të hakckerimeve me raste mashtrimi nga më të ndryshmet.

Shef i Sektorit të Hetimit të Krimit Kibernetik, Hergis Jica në një

2 https://www.statista.com/statistics/617136/digital-population-worldwide/.

3 G. R. G.Nikhita Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," International Journal of Engineering and Technology – UK, 2014.

intervistë tregon krimet më të shpeshta kibernetike për vitin 2021. "Vetëm në 3 mujorin e katërt të vitit që sapo lamë pas, kemi realizuar 4 operacione policore të gjitha të ndryshme nga njëra tjetra. Kemi pasur pornografi me të mitur, kërcënim të një punonjësi policie, kemi pasur rast mashtrimi kompjuterik dhe përgjim të paligjshëm apo ndërhyrje në të dhëna", -tregon shefi i sektorit të Krimit Kibernetik.

Krimi kibernetik është tani një nga sfidat më të mëdha ligjore.

Zhvillimi i Internetit ka qenë i hovëshm në nivel global dhe aktualisht rreth 4.95 billion njerëz janë online, 62.5 perqind e gjithe popullsise se botes[4]. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Tani pothuajse të gjitha krimet mund të kryhen me përdorimin e kompjuterave.

Pesha që zë krimi kibernetik në totalin e krimeve te rregjistruara në Shqiperi përgjatë vitit 2021 mbetet ende e ulet, por në krahasim me 2020-en vihet re një rritje e ndjeshme e tij.

Sipas raportit vjetor të Prokurosise së Përgjithshme, në 2021 veprat penale që lidhen me krimin kompjuterik u rriten me 0.25 përqind. Koeficenti i kriminalitetit për 100 mijë banorë për këtë grup veprash penal në vitin 2021 është 8.16, ndersa në vitin 2020 ka qenë 5.48.[5] Prokuroria thotë se në 2021, numri procedimeve te rregjstruara me akuzat qe lidhen me krimin kompjuterik është rritur me 48.08 përqind krahasuar me 2020, ka një rritje të numrit të procedimeve dërguar në gjykatë, nga 6 procedime në vitin 2020 në 10 procedime dërguar në gjykatë në vitin 2021 (66,67 %), rritje të numrit të të pandehurve të regjistruar në vitin 2021 përkundrejt këtij totali në vitin 2020 nga 3 në 25 (8,3 herë), rritje të numrit të të pandehurve të cilët janë dërguar në gjykatë nga 8 në 21 (2,6 herë) ndërsa numri i të pandehurve të dënuar për vepra penale kundër krimit kompjuterik nuk ka pësuar ndryshim, ngelet i njëjti 6[6].

Krimi kompjuterik cilësohet si krimi i njerëzve të arsimuar. Sipas raportit të Prokurorisë në lidhje me arsimin e të pandehurve rezulton se 73,68 % e tyre janë me arsim të mesëm, 15,79 % me arsim të lartë, 10,53 % me arsim deri 9-vjeçar. E vecanta është se të gjithë personat e marë të pandehur gjatë

4 G. R. G.Nikhita Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," International Journal of Engineering and Technology – UK, 2014.

5 Raport i Prokurorit te Pergjithshem mbi gjendjen e kriminalitetit per vitin 2021.

6 Raport i Prokurorit te Pergjithshem mbi gjendjen e kriminalitetit per vitin 2021.

2021 për këto akuza janë të pa dënuar më parë[7].

Ndërsa burime zyrtare në Policinë e Shtetit shpjegojnë se në Shqipëri përhapja e krimit kibernetik është në të njëjtat nivele me vendet e tjera, me diferencë zonat, ku nuk ka depërtim të internetit apo pajisjeve kompjuterike. "Shqipëria nuk bën dallim nga vendet e tjera dhe për këtë arsye, krimi kibernetik në vendin tonë ka një shtrirje të njëjtë, ashtu si dhe në vendet e tjera. Diferenca bëhet në zonat, ku nuk ka shtrirje të internetit apo në zonat, në të cilat nuk përdoren pajisje teknologjike të zgjuara, gjë që limitojnë dhe shtrirjen e krimeve kibernetike. Veprat më të përhapura janë mashtrimet kompjuterike, ndërhyrjet në sisteme, ndërhyrjet në të dhëna dhe falsifikimet kompjuterike, por nuk bëjnë përjashtim dhe veprat e tjera, të cilat mund dhe të ndërlidhen me këto mësipërme[8]

FBI kohët e fundit ka raportuar se numri i ankesave në lidhje me sulmet kibernetike në divizionin e tyre Kibernetik është deri në 4,000 në ditë. Shifrat janë marramendëse dhe të frikshme.Kjo përfaqëson një rritje prej 400% nga ajo që ata kanë parë para pandemisë COVID-19. Interpol po sheh gjithashtu një shkallë alarmante të sulmeve kibernetike që synojnë korporatat kryesore, qeveritë dhe infrastrukturën kritike. Këto sulme synojnë të gjitha llojet e bizneseve, por korporatat e mëdha, qeveritë dhe organizatat kritike mjekësore kanë qenë shënjestra kryesore.

Pra, siguria kibernetike është bërë një temë me rëndësi kombëtare, ndërkombëtare, ekonomike dhe shoqërore, e cila ndikon te të gjitha vendet.

Kjo lloj lufte, lufta kibernetike, rrit kërkesën për një forcë me kapacitet të fortë teknik, si p.sh., me aftësi në shkencat kompjuterike. Kjo kërkon zhvillimin e politikave, masa mbrojtëse dhe siguri për të trajtuar e zbutur kërcënimet kibernetike. Rreziqet ndaj sistemeve të komunikimit dhe të informacionit e kanë bërë mbrojtjen kibernetike, në fushën e sigurisë së vendit, një element që duhet marrë në konsideratë gjatë procesit të planëzimit dhe realizimit të operacioneve të sotme.

3. Rregulimi i krimit kibernetik në Shqipëri në kuadër të harmonizimit të legjislacionit të brendshëm me atë europian

Në legjislacionin Shqiptar deri në ndryshimet e e vitit 2008 nuk kanë

7 Raport i Prokurorit te Pergjithshem mbi gjendjen e kriminalitetit per vitin 2021.

8 Raporti i Policise se shtetit per vitin 2021.

qenë parashikuar vepra penale në fushen kompjuterike, edhe pse sistemet kompjuterike ishin bërë pjesë e shoqerisë shqiptare. Këtu përfshihet harmonizimi i legjislacionit kombëtar me atë ndërkombëtar për luften kundër krimeve kibernetike.[9]

Risit që paraqiste fusha perkatese dhe karakteristikat e veçanta të saj shtonin nevojen urgjente për një ndërhyrje normative e cila shtronte fushën e zbatimit të ligjit penal edhe ndaj sjelljeve kriminale të ndodhur në hapsirën kibernetike.

Një arsye tjetër që shtoj nevojen për shtimin e këtyre normave juridike-penale lidhej me nevojën e përafrimit të legjislacionit shqiptar me legjislacionin e Bashkimit Europian.

Për të bërë të mundur këtë Republika e Shqipërisë ratifikoj "Konventa për Krimin Kibernetik" me Ligjin Nr 8888 datë 25.04.2002. Më pas në vitin 2004 ka ratifikuar dhe protokollin shtesë të kësaj konvente.

Pra në këtë mënyrë dispoziatat e perfshira në Kodin Penal për këto krime janë në koherencë të plotë me parashikimet e Konventës së Këshillit të Europës "Mbi Krimin Kibernetik".

Gjithashtu duhet thënë se kjo përvecse ndihmon Shqipërin në synimin për plotësimin e detyrimeve që lidhen me integrimin në familjen europiane por edhe në nevojën e krijimit të koncepteve uniforme dhe vendosjen e standarteve të përbashkëta të bashkëpunimit për të luftuar një fenomen me natyrë ndërkombëtare.

Për të reflektuar angazhimet e Shqipërise në kuader të Konventes të Krimit Kibernetik, Ministria e Drejtësisë mori nismën për parashikimin e shtesave në Kodin Penal të Republikës së Shqipërisë dhe Kodin e Procedurës Penale. Keto nisma u finalizuan respektivisht me miratimin e ligjit nr. 10023, datë 27.12.2008 dhe nr. 10054 datë 29.12.2008.

Duhet thënë se Kodi Penal përpara shtesave me ligjin 10023\2008 parashikonte në nenin 192\b1 të tij si vepër penale ndërhyrjen në transmetimet kompjuterike. Por kjo dispozite sipas ekspertëve shqiptarë dhe të huaj, ishte e karakterit te përgjithshëm, përmbajtja e saj nuk i përgjigjej dhe nuk mbulonte në mënyrë të mjaftueshme sferen e atyre veprimeve, të cilat për nga natyra e tyre përmbajnë tipare dhe karakteristika objketive të dallueshme nga njëra-tjetra.

9 Denisa.A "*Mbi disa ceshtje te se drejtes penale dhe proceduriale*" fq 46.

3.1 Shpërndarja kompjuterike pro genocidit ose krimet kundër njerëzimit

Neni 74/a[10] është shtuar në Pjesën e Posacme të Kodit Penal.

Objekti janë mardhëniet juridike të vendosura me ligj në Republikën e Shqipërisë që kanë të bejnë me mbrojtjen e jetës shëndetit dhe të drejtave e lirive të publikut. Për shkak të objektit që mer në mbrojtje kjo vepër penale, ajo është pozicionuar në Kreun 1 "*Krime kundër njeëezimit*". Nisur nga rrezikshmëria e kësaj vepre ajo është parashikuar si krim dhe sanksioni penale varjon nga tre gjer në gjashtë vjet.

Nga ana objektive krimi kryhet në forma dhe mënyra të cilat janë specifikuar në nenin 74/a:

1. Ofrimi në publik ose shpërndarja publikut e materjaleve që përbejnë genocid ose krime kundër njerëzimit. (ka karakter masiv)
2. Ofrimi ose shpërndarja e materialeve realizohet me menyra dhe mjete të posacme. (nëpermjet sistemeve kompjuterike)
3. Këto materiale mohojnë, minimizojnë, miratojnë ose justifikojnë akte, që përbëjnë gjenocid ose krim kundër njerëzimi.

Për konstatimin e krimit nuk kerkohet ardhja e pasojave si pasoja morale, psikologjike pra pasoja jomateriale.

Subjekt i krimit mund të jetë cdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm, i cili i *ofron* dhe *shpërndan* materiale publikut. Nga kjo kuptojmë që subjekti mund të jetë burimi fillestar nëpermjet ofrimit ose burimi dytësor nëpërmjet shpërndarjes së materialeve. Gjithashtu vem re se ky veprim duhet ti adresohet një numri personash që konsiderohet "publik". Në jurisprudencën gjyqësore nuk kemi një përkufizim të saktë se cfarë do të quajm publik, sa është minimumi i personave që bëjnë ate që quhet "publik".

Ana subjektive kërkohet ekzistenca e fajit në formën e dashjes, pra me dashje direkte dhe qëllim të caktuar. Motivet nuk kanë rëndësi për cilësimin e krimit.Përmendem më siper se mjeti i ofrimit dhe i shpërndarjes së materialeve është sistemi kompjutrik. Përkufizimi i sistemit kompjuterik

10 Neni 74/a "**Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit"** "Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve, që mohojnë, minimizojnë, në mënyrë të ndjeshme, miratojnë ose justifikojnë akte, që përbëjnë gjenocid ose krim kundër njerëzimit, dënohet me burgim tre deri në gjashtë vjet".

është dhënë në Konventën për Krimin Kibernetik, sipas të cilës "sistem kompjuterik" do të thotë cdo lloj pajisje apo grup i nderlidhur ose pajisje te lidhura, nje ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

Gjithashtu persa i përket anës subjektive duhet thënë se përmbajtja e materialeve tregon mendimin e autorit pro veprës penale të genocidit dhe krimeve kundër njerzimit. Nëse mohimi, miratimi ose justifikimi i këtyre akteve është lehtësisht i kuptueshëm tek "minimizimi" ligjvënësi ka parashikuar që duhet të jetë në mënyrë të ndjeshme, e dukshme.

3.2 Neni 84/a "Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik"[11]

Objekti. Për shkak të objektit që mer në mbrojtje kjo dispozitë është pozicionuar në Kreun II të Pjese së Posacme të Kodit Penal "Vepra penale kunder jetës". Konkretisht objekt i krimit janë marrëdheniet juridiket te vendosura për të mbrojtur jeten dhe shëndetin e personit qei përket një etnie, kombësie, race apo feje të caktuar. Veç motivit, figura e kanosjes cilësohet në këtë dispozitë edhe për shkak të mjetit të kryerjes së veprës penale nëpërmjet sistemit komjuterik, për të cilin vlejnë shpjegimet e dhëna mbi nenin 74/a[12].

Nga ana objektive, krimi kryhet me veprime aktive kanosje serioze nëpërmjet sistemeve kompjuterike, kanosja është serioze për vrasje ose plagosje të rëndë.

Subjekt i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive, krimi kryhet me dashje direkte dhe per motive racizmi ose ksenofobie. Ne kuptimin e ngushte "racizmi" ndryshon nga "ksenofobia". Racizmi bazohet në dallimin racor, ndërsa ksenofobia bazohet në dallimin për shkak të qënies i huaj.

3.3 Neni 119/a Shpërndarja e materialeve raciste ose

11 **"Kanosja me motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik"** Kanosja serioze për vrasje ose plagosje të rëndë, që i bëhet një personi, nëpërmjet sistemeve kompjuterike, për shkak përkatësie etnike, kombësie, race apo feje, dënohet me gjobë ose me burgim deri në tre vjet.

12 Neni 74/a i Kodit Penal

ksenofobike nëpërmjet sistemit kompjuterik [13]

Kjo dispozite dhe ajo pasardhese eshte pozicionuar në Kreun II të Pjesës së Posaçme të Kodit Penal - Vepra penale kundër jetës, per shak se qëllimi i këtyre dispozitave është mbrojtja e dinjitetit dhe personalitetit të personave të cilët i përkasin një etnie, kombësie, race apo feje të caktuar.

Objekti është objekt i posaçëm, pra janë marrëdhëniet juridike të vendosura për të siguruar ndjenjën e dinjitetit personal të personave që u përkasin racave të tjera.

Nga ana objektive, figura e veprës penale kryhet me anë të ofrimit ose të shpërndarjes publikut me anë të sistemeve kompjuterike të materialeve me përmbajtje raciste ose ksenofobike. Kjo formë ka karakter masiv dhe përmbajtja e këtyre materialeve ka karakter fyes, poshtërues, ksenofobike, përçmuese, frikësuese për personat e racave të tjera.

Subjekt i figurës së veprës penale mund të jetë çdo person që ka mbushur moshën dhe është i përgjegjshëm, i cili ofron ose shpërndan materiale me përmbajtje raciale ose ksenofobike, publikut.

Nga ana subjektive kjo vepër kryhet me dashje direkte dhe me qëllim i cili është i posaçëm, racist ose ksenofobik.

3.4 Neni 119/b "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik"[14]

Objekti është gjithashtu objekt i posaçëm, sepse ka të bëjë me nderin e dinjitetin e personave të veçantë që u përkasin një race, kombësie, etnie apo feje të caktuar.

Nga ana objektive vepra penale kryhet me anë të sistemit kompjuterik, fyerjes publikisht, pra ka karakter masiv.

Subjekt i veprës penale të fyerjes mund të jetë çdo person që ka mbushur

13 Neni 119/a, **Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik** *Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve me përmbajtje raciste ose ksenofobike përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.*

14 Neni 119/b, **Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik** *Fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.*

moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive kjo vepër kryhet me dashje direkte ndaj një personi për motive racizmi ose ksenofobie.

Përsa i takon ketij neni duhet vënë në dukje që me ligjin nr. 10054, datë 29.12.2008 —Për disa shtesa dhe ndryshime në Kodin e Proçedurës Penale, është parashikuar që në nenin 59 të Kodit të Proçedurës Penale ndër veprat penale që ndiqen me ankim të të dëmtuarit akuzues të jetë edhe fyerja me motive racizmi e ksenofobie. Kjo shtesë ka patur si qëllim për të harmonizuar shtesat në Kodin Penal, i cili veprat penale mbi fyerjen ndaj një personi konkret i përfshin në rrethin e çështjeve që ndiqen vetëm me ankimin e të dëmtuarit akuzues, i cili edhe mund ta tërheqë atë gjatë proçedimit[15].

3.5 Neni 143/b "Mashtrimi kompjuterik"[16]

Objekti Me anë të kësaj dispozite synohet që të mbrohet pasuria e personave nga ndërhyrjet kompjuterike që u bëhet sistemeve të tyre. Meqë objekti kryesor i marrë në mbrojtje nga kjo dispozitë janë marrëdhëniet juridike të vendosura në sferën e sigurisë së të drejtës së pronësisë private ose publike të shtetit të mbrojtura nga legjislacioni penal nga veprimet ose mosveprimet kriminale, kjo dispozitë është pozicionuar në Kreun III të Pjesës së Posaçme - Vepra penale kundër pasurisë.

Për të siguruar që të mbuloheshin të gjitha manipulimet e mundshme, krahas elementëve: futja, ndryshimi, fshirja ose heqja, teksti i kësaj norme përmban edhe fjalët "ndërhyrja në funksionimin e një sistemi komjuterik" që tregon një veprim të përgjithshëm.

Nga ana objektive krimi kryhet në forma dhe mënyra të ndryshme:

a. Me anë të futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike;

15 Neni 284 të K.Pr.Penale.

16 Neni 143/b- **Mashtrimi kompjuterik**

Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet dhe me gjobë nga 60 000 (gjashtëdhjetë mijë) lekë deri në 600 000 (gjashtëqind mijë) lekë.

Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet dhe me gjobë nga 500 000 (pesëqind mijë) lekë deri në 5 000 000 (pesë milionë) lekë.

b. Me anë të ndërhyrjes në funksionimin e një sistemi kompjuterik.

Në të gjitha rastet kërkohet ardhja e pasojave kriminale, dëmi material i shkaktohet një personi ose më shumë personave.

Subjekti i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive krimi kryhet me dashje te drejtëpërdrejtë për të marrë pasurinë e personit fizik, personit juridik apo shtetëror me qëllim për të nxjerrë përfitime materiale për vete ose për persona të tjerë.

Rrethanat cilësuese janë:

a) Me mashtrim të kryer në bashkëpunim (krimi kryet nga dy ose më tepër persona në marrëveshje midis tyre) ;

b) Me mashtrim te kryer në dëm të disa personave, (kur janë mashtruar dy, tre ose më tepër persona në kohë të ndryshme) ;

c) Me mashtrim të kryer më shumë se një herë, (veprimi i kryer për disa kohë kur personi ka mashtruar disa herë persona të ndryshëm, ose edhe të njëjtin person në interval kohor të shkurtër por nuk është dënuar për krimin e parë dhe vendimi nuk ka marrë formën e prerë);

d) Me mashtrim kur ka sjellë pasoja të rënda, (mashtrimi në përmasa të mëdha).

Më konkretisht lidhur me fgurën e veprës penale të parashikuar nga neni 143/b/1 të K.Penal është shprehur edhe Gjykata e Lartë në çështjen me palë: Prokuroria e rrethit Gjyqësor Tiranë kundër shtetasve me iniciale XH.G, M.P, A.K, E. SH, S.SH, S.K[17]. Për vlerësimin e përgjegjësisë penale të të gjykuarve gjykata ka analizuar në mënyrë të veçantë elementin e figurës te veprës penale në referim të nenit 143/b/1 të K.Penal

17 Vendim i Gjykatës së lartë Nr.00-2013-1587 (261), datë 02.10.2013.

3.6 Neni 186/a "Falsifikimi kompjuterik"[18]

Specifike për këtë vepër penale është që veprimet e futjes, ndryshimit, heqjes apo fshirjes së të dhënave kompjuterike të jenë kryer pa të drejtë. Kjo reflekton idenë që një sjellje e tillë nuk është gjithnjë e dënueshme, por mund të jetë e ligjshme ose e justifikuar si rast i ushtrimit të një të drejte.

Objekt i krimit janë marrëdhëniet juridike të vendosura për të siguruar interesat publik, të mbrojtura nga legjislacioni penal. Në këtë figurë falsifikimi kryhet në kompjuter, kundër interesit publik.

Nga ana objektive, krimi kryhet me forma e mënyra të ndryshme si futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike.

Subjekt. Në paragrafin e parë subjekti i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm dhe që kryen krimin e falsifikimit kompjuterik. Në paragrafin e dytë ku parashikohen rrethanat e cilësuara, subjekti është i posaçëm, janë personat që kanë për detyrë ruajtjen ose administrimin e të dhënave kompjuterike.

Nga ana subjektive krimi kryhet me dashje të drejtëpërdrejtë dhe me qëllim paraqitje ose përdorimin e të dhënave si autentike

3.7 Neni 192/b "Hyrja e paautorizuar kompjuterike"[19]

Me anë të kësaj dispozite synohet të mbrohet përmbajta e të dhënave kompjuterike nga aksesi i paautorizuar. Hyrja e paautorizuar është një vepër penale e cila konsumohet vetëm me kryerjen e veprimit të hyrjes në sistem dhe njohjes me të dhëna që përmban sistemi, duke mos përjashtuar mundësinë që autori i veprës të përgjigjet për veprat e tjera sipas parashikimeve të neneve te tjera.

---

18 Neni 186/a, **Falsifikimi kompjuterik**
Futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet. Kur kjo vepër kryhet nga personi, që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike, në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda për interesin publik, dënohet me burgim tre deri në dhjetë vjet.

19 Neni 192/b- **Hyrja e paautorizuar kompjuterike**
Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

Objekt i krimit janë marrëdhëniet juridike të vendosura për të siguruar rregullsinë dhe saktësinë e programeve kompjuterike në dëm të interesave të personave ose ato publike.

Nga ana objektive krimi kryhet në forma dhe mënyra të ndryshme, me hyrje të paautorizuar apo me tejkalim të kompetencave për të hyrë në një sistem kompjuterik ose në një pjesë të tij, nëpërmjet cënimit të masave të sigurimit.

Subjekt i krimit është i përgjithshëm ose i posaçëm.

Nga ana subjektive krimi kryhet me dashje të drejtpërdrejtë. Rrethanat cilësuese të krimit janë kur ai kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetsisë apo në çdo sistem tjetër kompjuterik me rëndësi publike. Këto rrethana përfundojnë me hipotezën —çdo sistem tjetër kompjuterik me rëndësi publike‖ duke lënë të hapur per pushtetin gjyqësor elaborimin e këtij koncepti për zgjidhjen e rasteve që mund të ndeshen në praktikë.

3.8 Neni 293/a "Përgjimi i paligjshëm i të dhënave kompjuterike"[20]

Kjo vepër penale dhunon privatësinë e komunikimit në të njëjtën mënyrë si përgjimi tradicional dhe regjistrimi i bisedave telefonike midis personave. E drejta e privatësisë përbën të drejtë themelore të sanksionuar nga Kushtetuta jonë, si dhe nga neni 8 i Konventës Evropiane të të Drejtave të Njeriut.

Objekti i krimit janë marrëdhëniet juridike të vendosura për të siguruar paprekshmërine e të dhënave kompjuterike nga çdo mjet apo mënyrë.

Nga ana objektive krimi kryhet me anë të përgjimit të paligjshëm, me mjete teknike të transmetimeve jopublike të të dhënave kompjuterike, përfshirë emetimet elektromagnetike ose nga një sistem kompjuterik që mban të dhëna kompjuterike.

Subjekt i krimit mund të jetë çdo person që kryen përgjim të paligjshëm të të dhënave kompjuterike.

---

20 Neni 293/a- **Përgjimi i paligjshëm i të dhënave kompjuterike**
Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet.

Nga ana subjektive krimi kryhet me dashje. Rrethanat e cilësuara janë kur krimi kryhet brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndesi publike.

3.9 Neni 293/b "Ndërhyrja në të dhënat kompjuterike, ndërhyrja në sistemet kompjuterike, keqpërdorimi i paisjeve"[21]

Objekti i krimit janë marrëdhëniet juridike të vendosura për të siguruar paprekshmërine e të dhënave kompjuterike nga çdo mjet apo mënyrë.

Nga ana objektive krimi kryhet nëpërmjet dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të paautorizuar të të dhënave kompjuterike.

Subjekt i krimit mund të jetë çdo person që kryen përgjim të paligjshëm të të dhënave kompjuterike.

Nga ana subjektive krimi kryhet me dashje.

3.10 Neni 293/c "Ndërhyrja në sistemet kompjuterike"[22]

Objekti i krimit janë marrëdhëniet juridike të vendosura për të siguruar funksionimin e sistemit kompjuterik nga ndërhyrje të mbrojtura nga legjislacioni penal.

Nga ana objektive krimi kryhet me ndërhyrje në sistemin kompjuterik nëpërmjet krijimit të pengesave serioze, futjes, dëmtimit, shtrembërimit,

---

21 Neni 293/b, **Ndërhyrja në të dhënat kompjuterike**
Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet. Kur kjo vepër kryhet në të dhënat kompjuterike ushtarake, të sigurisë. kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

22 *Neni 293/c, **Ndërhyrja në sistemet kompjuterike***
Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.

ndryshimit, fshirjes apo suprimimit të të dhënave.

Subjekt i krimit mund të jetë çdo person që krijon pengesa serioze dhe cënon funksionimin e një sistemi kompjuterik.

Nga ana subjektive krimi kryhet me dashje.

Konkluzione dhe rekomandime

Shoqëritë në mbarë botën janë të tërhequra ndaj përfitimeve të mëdha që sjell teknologjia e informacionit dhe komunikimit dhe qeveritë në vendet e zhvilluara po investojnë në këtë fushë. Këto përfitime që i kalojnë shtetit dhe qytetarëve të tij kanë nevojë të mbrohen nga sulmet kibernetike, sepse kanë rëndësi për sigurinë e vendit.

Hapësira kibernetike si një hapësirë pa kufinj kërkon një bashkëpunim dhe koordinim ndërkombëtar për të garantuar sigurinë kibernetike. Gjithashtu me anëtarësimin në NATO dhe progresin e bërë drejt anëtarësimit në BE, Shqipëria gjithnjë e më shumë është pjesë aktive e iniciativave dhe programeve të sigurisë kibernetike dhe duhet të përmbushë angazhimet e saj ndaj vendeve aleate. Shqipëria duhet të marrë të gjitha masat për hartimin e politikave, standardeve, udhëzimeve dhe procedurave bazuar në standardet dhe praktikat më të mira për të garantuar sigurinë kibernetike, për të siguruar një mbrojtje ndaj rreziqeve kibernetike duke respektuar në çdo moment parimet e të drejtave dhe lirive themelore si dhe parime të tjera demokratike.

Në Shqipëri, Agjensitë publike dhe private nuk çertifikohen nën standartet të cilat njihen nderkombëtarisht. Brënda institucioneve publike, trajnimi për sigurinë kibernetike si për stafin e IT, edhe për atë në përgjithësi, janë shumë të limituara dhe shpesh varen nga menaxhimi i institucionit. Gjithashtu, duhet sa më shpejt të kërkohet që mbrojtja nga sulmet kibernetike, të behet pjesë e kurikulave nëpër shkolla dhe të jepen udhëzime veçanërisht për fëmijët, që bien shpesh pre e abuzimeve nëpër rrjete të ndryshme.

Edhe pse ligjvënësi shqiptar ka bërë përpjekje të shumta për t‘iu përgjigjur krimit kibernetik duke përfshirë në Kodin Penal dispozita të veçanta për forma të veçanta të këtij lloj kriminaliteti, konstatohet se dispozitat aktuale janë të shpërndara në mënyrë jo sistematike në krerë e seksione të ndryshme të Kodit Penal.

Në këtë kuadër për lehtësimin e zbatimit praktik dhe rrijen e efektivitetit të tyre do të ishte mirë që të tilla vepra penale të përfshiheshin në një ligj të veçantë.

Bibliografia

Kodi Penal i Republikës së Shqipërisë https://qbz.gov.al/preview/a2b117e6-69b2-4355-aa49-78967c31bf4d

Kodi i Procedurës Penale i Republikës së Shqipërisë https://qbz.gov.al/preview/b4819f4d-c246-49b3-87a9-2e6c8512c975

techtarget.com/searchsecurity/definition/cybercrime

Raporti rajonal CARPO https://rm.coe.int/16806ef3d4

https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

https://www.shish.gov.al/pages/lajme/siguria2020.html

https://www.pp.gov.al/Dokumente/RAPORTE_T_PROKURORIT_T_P_RGJITHSH_M/

https://www.statista.com/statistics/617136/digital-population-worldwide/

Vendim i Gjykatës së lartë Nr.00-2013-1587 (261), datë 02.10.2013

Ligji nr. 10023, dt. 27.11.2008 —*Për disa shtesa dhe ndryshime në Kodin Penal të R.SH*

Ligji nr. 8888, dt. 25.04.2002 "*Për Ratifikimn e Konventës për Krimin në fushën e Kibernetikës"*

"Trajnim për krimin kibernetik për gjyqtarë dhe prokurorë: një koncept", Departamenti i Shoqërisë së Informacionit dhe Aksionit kundër Krimit Drejtoria e Përgjithshme e të Drejtave të Njeriut dhe Çështjeve Ligjore Strasburg www.coe.int/cybercrime.

COPYRIGHT INFRINGEMENTS AND ADMINISTRATIVE PROTECTION

ENEA SHEQI[1]

INA HASANKOLLI[2]

Abstract

Copyright protection in today's reality faces many challenges and difficulties. Technological developments have made copyright infringements of various forms and their identification is very difficult. Authors to protect their creations can address violations of their works in courts, or they can request a criminal investigation. But in addition to the protection of copyright in civil and criminal terms there is also the protection of copyright in administrative terms. This protection refers to cases when the state through its institutions invests to protect creators and their literary, artistic and scientific creations. This paper will address the legal framework in force in relation to copyright infringements and administrative offenses, as well as the institutions involved in terms of respect for copyright and other related rights. The paper also provides an overview of national and international jurisprudence of copyright intertwined with international legislation in terms of respect for intellectual property rights.

Key words: copyright, infringement, offenses, administrative pro

1 Inspector, State Inspectorate of Market Surveillance, contact: enea.sheqi@yahoo.com

2 Legal expert, General Directorate of Taxation, contact: inahasankolli@yahoo.com

CËNIMI I TË DREJTËS SË AUTORIT DHE MBROJTJA E SAJ NË ASPEKTIN ADMINISTRATIVE

Abstrakt

Mbrojtja e të drejtës së autorit në realitetin e sotëm has në shumë sfida dhë vështirësi. Zhvillimet teknologjike kanë bërë që shkeljet e së drejtës së autorit të jenë nga format më të ndryshme dhe identifikimi i tyre të bëhet me shumë vështirësi. Autorët për të mbrojtur krijimet e tyre mund të investohen gjyqësisht për të trajtuar shkeljet që i bëhen veprave të tyre, apo mund të kërkojnë dhe një hetim penal. Por krahas mbrojtjes të së drejtës së autorit në aspektin civil dhe penal ekziston dhe mbrojtja e së drejtës së autorit në aspektin administrativ. Kjo mbrojtje i referohet rasteve kur shteti nëpërmjet institucioneve të tij investohet për të mbrojtur krijuesit dhe krijimet e tyre letrare, artistike dhe shkencore. Në këtë punim do të bëhet një trajtim i kuadrit ligjor në fuqi në lidhje me shkeljet e së drejtës së autorit dhe kundravajtjet administrative, si dhe institucioneve të përfshira në drejtim të respektimit të të drejtave të autorit dhe të drejtave të tjera të lidhura me to. Gjithashtu në punim bëhet një pasqyrim i jurisprudencës kombëtare dhe ndërkombëtare e të drejtës së autorit të ndërthurur me legjislacionin ndërkombëtar në drejtim të respektimit të të drejtave të pronësisë intelektuale.

Fjalë kyçe: e drejta e autorit, cënim, mbrojtje administrative, kundravajtje

I. Hyrje

Pronësia intelektuale në kuptimin e ngushtë të saj përfshin të drejtat ligjore që rrjedhin nga aktiviteti intelektual në fushën e industrisë, shkencës, artit e letërsisë.[3] Termi pronësi intelektuale i referohet gjerësisht krijimeve të mendjes së njeriut. Të drejtat e pronësisë intelektuale mbrojnë interesat e krijuesve duke ju dhënë atyre të drejtën e pronës mbi krijimet e tyre.[4] Pronësia intelektuale mund të përkufizohet edhe si e drejta ligjore mbi

3 WIPO, *WIPO Intellectual Property Handbook: Policy, Law and Use*, Second Edition, 2008, fq.3.

4 Drejtoria për të Drejtën e Autorit, *Të kuptojmë të drejtën e autorit dhe të drejtat e tjera të lidhura me të,* Broshurë, fq.5.

krijimtarinë intelektuale.[5]

Nëse do i referoheshim ndarjeve të degës së Pronësisë Intelektuale sipas doktrinës, atëherë dy ndarjet më të mëdha të saj janë: "E drejta e autorit" dhe "Pronësia industriale"[6]. Në të drejtën e autorit përfshihen të gjitha ligjet ose aktet ligjore të cilat mbrojnë të drejtat e krijuesve të veprave letrare, artistike dhe shkencore. Ndërsa në të drejtën e pronësisë industriale gjenden të gjitha normat të cilat mbrojnë shpikjet (patentat), dizenjot industriale, markat tregtare, treguesit gjeografikë, modelet e përdorimit, etj. Në vitet e fundit krahas këtyre ndarjeve të sipërpërmendura janë shfaqur edhe një grup të drejtash të tjera të pronësisë intelektuale të mbrojtura, të quajtura ndryshe "*sui generis*". Me anë të këtyre të drejtave synohen që të mbrohet varieteti i bimëve, të drejtat e gjysmë-përçuesve topografikë, etj.

E drejta e autorit është një tërësi të drejtash ligjore e cila merret me mbrojtjen e të drejtave të krijuesve mbi veprat letrare apo artistike.[7] Qëllimi i së drejtës së autorit është të promovojë kulturën, artin dhe zhvillimin teknologjik e shkencor. Kjo bëhet duke shpërblyer autorët për krijimet e punimet e tyre, si dhe duke ruajtur një balancë ndërmjet autorëve, sipërmarrësve (botues, transmetues, prodhues fonogrami etj) dhe interesit publik[8]. Të drejtat ekonomike të autorit e lejojnë atë që të përfitojë nga riprodhimi apo nga shfrytëzimi i veprës së tyre. Krijimet e autorit në të shumtën e legjislacioneve të shteteve të ndryshme njihen me emrin ***"vepër".***[9]

E drejta e autorit është një e drejtë pronësie dhe ashtu si çdo e drejtë pronësie mund që të transferohet dhe të kalohet tek një peson tjetër, së bashku me disa të drejta që rrjedhin nga kjo e drejtë.[10]

E drejta e autorit ka dhe një qëllim tjetër të rëndësishëm, atë të pasurimit të kulturës dhe të shoqërisë me informacion.[11] Mbrojtja e siguruar nga e drejta e autorit për përpjekjet e shkrimtarëve, artistëve, stilistëve, dramaturgëve,

5 Fatos Dega, *Pronësia Intelektuale*, Botimi i IV, Morava, Tiranë, 2014, fq.20.

6 Tate Legal, *A brief Guide to Copyright*, August, 2016, fq.6.; Fatos Dega, *Pronësia Intelektuale*, Botimi i IV, Morava, Tiranë, 2014, fq.21.

7 WIPO, *Advanced Course on Copyright and Related Rights,* Module I: The Concept of Copyright, the Historical Background and the International Framework, Geneva, 2019, fq-3-6.

8 WIPO, *Advanced Course on Copyright and Related Rights,* Module I: The Concept of Copyright, the Historical Background and the International Framework, Geneva, 2019, fq-3-6.; Fatos Dega, *Pronësia Intelektuale*, Botimi i IV, Morava, Tiranë, 2014, fq.24.

9 Paul Torremans, *Holyak & Torremans Intellectual Property Law*, 7th Edition, Oxford University Press, UK, 2013, fq.196.

10 Tate Legal*, A brief Guide to Copyright*, August, 2016, fq.6.

11 Robert A. Gorman, *Copyright Law, Federal Judicial Center*, 2006, fq.1.

muzikantëve, arkitektëve, prodhuesve të tingujve apo të filmave, ose të programeve kompjuterike, siguron një atmosferë të favorshme për krijimtarinë, e cila i shtyn ata që të krijojnë më shumë dhe të motivojnë të tjerët në të njëjtën kohë.[12]

II. Zbatimi i të drejtave të autorit dhe masat për mbrojtjen e saj

Zbatimi i të drejtave të autorit nënkupton të gjitha ato masa që ndërmerren në rastet kur kemi shkelje apo cënim të së drejtës së autorit apo të drejtave të tjera të lidhura me to.[13] Zbatimi i të drejtave të autorit ka pasur një evolucion galopant vitet e fundit për shkak të ndryshimeve teknologjike duke përfshirë këtu teknologjinë digjitale, e cila lejon që shumë vepra të transmetohen apo të kopjohen pa kurrëfarë kontrolli. Një tjetër arsye në lidhje me krijimin e një sistemi të zbatimit të të drejtave të autorit është dhe fakti se këto mallra dhe shërbime të mbrojtura nga e drejta e autorit kanë një impakt ekonomik në tregun e brendshëm dhe atë ndërkombëtar.[14]

Akti kryesor në lidhje me zbatimin e të drejtave të autorit mbetet Marrëveshja "Mbi disa aspekte të lidhura me tregtinë e pronësisë industriale" (TRIPS), në të cilën shtetet kontraktuese detyrohen që të vendosin masa për të mbrojtur të drejtën e autorit dhe të drejtat e tjera të lidhura me to. Masat kryesore në lidhje me mbrojtjen e të drejtat e autorit janë:[15]

- Masat civile;
- Masat penale;
- Masat administrative.

Të drejtat e autorit dhe të drejtat e tjera të lidhura me to i japin palëve të drejta civile të cilat në shumë juridiksione konsiderohen edhe si të drejta pronësie. Pra, nëse kemi të bëjmë me shkelje të këtyre të drejtave, në thelb kemi të bëjmë me shkelje apo cënim të pronës.[16] Por, ashtu siç e dimë nga

12 The Institute of Company Secretaries of India, *Intellectual Property Rights-Law and Practice*, Study Material, New Dehli, fq.147.

13 Aaron Schwabach, *Intellectual Property: A Reference Handbook*, ABC-CLIO, England, 2007, fq.21.

14 WIPO, *WIPO Intellectual Property Handbook*, Geneva, 2004, fq.213.

15 WIPO, *Advanced Cource on Copyright and Related Rights*, Module 8: The TRIPS Agreement and Enforcement Issues , WIPO, 2019, Geneva, fq.17.

16 Jennifer Davis, *Intellectual Property Law,* 4th Edition, Oxford University Press, Hampshire, 2012, fq.13.

kalimi i të drejtave të autorit, forma e kalimit të tyre është ajo kontraktuale dhe kur një palë e cila nuk ka zbatuar apo respektuar kontratën mbi kalimin e të drejtave pasurore janë veprime të cilat përbëjnë shkelje të kontratës. Për këto veprime mund të ngrihen padi civile në gjykatat civile ose në gjykatat tregtare në disa juridiksione të tjera. Në thelb këto janë masat civile për mbrojtjen e të drejtës së autorit dhe të drejtave të tjera të lidhura me to.[17] Pra, në rastet kur nuk arrihet marrëveshja mes palëve si rrugë për të mbrojtur të drejtat e autorit mbetet gjykimi civil. Në gjykimet civile në rastet kur kërkohet njohja e shkeljes të së drejtës së autorit mund të pretendohet edhe një masë dëmshpërblimi për autorin.[18] Dëmshpërblimi mund të variojë si dëm ekonomik ashtu edhe në rastet kur pretendohet se palës i është shkaktuar një dëm moral.[19]

Masat penale giithashtu luajnë një rol të rëndësishëm në mbrojtjen e të drejtave të pronësisë intelektuale. Këto masa vendosen në rastet kur kemi të bëjmë me shkelje të cilat shihen serioze nga pikëpamja e politikave publike. Për shembull, pothuajse në të gjitha legjislacionet e shteteve përcaktohen dënime penale për veprimet e piraterisë të së drejtës së autorit.[20] Legjislacionet penale përcaktojnë mbrojtje si për të drejtat ekonomike dhe për ato morale, duke përcaktuar edhe dispozita specifike në lidhje me cënimin e të drejtave përkatëse të autorit.[21]

Së fundmi masat administrative luajnë një rol të rëndësishëm në ruajtjen e standarteve të tregtisë dhe rol ndihmës në ruajtjen dhe zbatimin e të drejtave të pronësisë intelektuale. Për shembull autoritetet doganore kryejnë veprimtarinë administrative në kufi për të parandaluar rastet e piraterisë së të drejtave të autorit. Me kërkesë të mbajtësit të së drejtës autoritetet administrative mund që të kryejnë ndalime të importeve të cilat shkelin të drejtat e autorit, apo në vendet ku kryhen inspektime të parandalojnë kryerjen e shkeljeve të të drejtave të autorit.[22] Mbrojtja në nivel administrativ

17 WIPO, *Advanced Cource on Copyright and Related Rights*, Module 8: The TRIPS Agreement and Enforcement Issues , WIPO, 2019, Geneva, fq.18.

18 Jennifer Davis, *Intellectual Property Law*, 4th Edition, Oxford University Press, Hampshire, 2012, fq.71.

19 Uarda Albunesa, *E drejta e autorit në shëipëri dhe në legjislacionin europian; përqasja mes tyre*, Doktoratura, Tiranë, 2014, fq.71.

20 WIPO, *Advanced Cource on Copyright and Related Rights*, Module 8: The TRIPS Agreement and Enforcement Issues , WIPO, 2019, Geneva, fq.19.

21 Uarda Albunesa, *E drejta e autorit në shqipëri dhe në legjislacionin europian; përqasja mes tyre*, Doktoratura, Tiranë, 2014, fq.74.

22 WIPO, *Advanced Cource on Copyright and Related Rights*, Module 8: The TRIPS Agreement and Enforcement Issues , WIPO, 2019, Geneva, fq.20.

konsiderohet ndryshe edhe si një investim i shtetit për të mbrojtur krijimtarinë letrare, artistike dhe shkencore në vend.[23]

Traktatet ndërkombëtare që adresojnë çështje të së drejtës së autorit japin disa mekanizma në lidhje me mbrojtjen e së drejtës së autorit të cilat janë të inkorporuara pothuajse në legjislacionin e të gjitha vendeve anëtare. Këto mekanizma mund të jenë:[24]

· Sekuestrimi i kopjeve që cënojnë të drejtën e autorit (të paligjshme). Ky është një parashikim ligjor i gjendur në Konventën e Bernës, por edhe në Marrëveshjen TRIPS[25]. Më së shumti mund të themi se ky detyrim i referohet kopjeve fizike sesa atyre digjitale.

· Urdhëri për të ndaluar shkeljen e së drejtës së autorit. Mbajtësi i së drejtës së autorit mund që ti kërkojë gjykatës nxjerrjen e një urdhëri të tillë me qëllim ndalimin e vazhdimit të cënimit të së drejtës së autorit. Ajo çka favorizon këtë urdhër është shpejtësia kohore dhe mundësia për të parandaluar vazhdimin e humbjeve ekonomike. Një parashikim i tillë gjendet në nenin 44 të Marrëveshjes TRIPS.

· Shpërblimi për shkaktimin e dëmit. Kjo është një e drejtë e parashikuar në nenin 45 të Marrëveshjes TRIPS, duke mundësuar mbajtësin e së drejtës që të kërkojë shpërblimin për shkaktimin e dëmit për shkeljen e së drejtës së autorit. Megjithëse në dukje duket e leverdisshme, kjo kërkesë mbart edhe disa problematika që kanë të bëjnë me caktimin e sasisë së dëmit të pësuar dhe mundësisë për të paguar këto dëmshpërblime. Për shembull, nëse ndodh një publikim i paautorizuar i një vepre në internet është shumë e vështirë që të përcaktohet sesa dëm i është shkaktuar mbajtësit të së drejtës. Gjithashtu do të ishte më e vështirë për të paraqitur një kërkesë të tillë përballë çdo personi që mund të kryejë një shkelje të së drejtës së autorit, pasi mund të ndodhë që ky person të mos ketë asnjë aset.

· Dënimet penale. Në të shkuarën dënimet (sanksionet) penale i atribuoheshin personave të cilët nixrrnin përfitime ekonomike nga shkelja e së drejtës së autorit, por Marrëveshja TRIPS[26] dhe zhvillimet e reja të legjislacionit penal bënë që të dënoheshin veprimet e cënimit të së drejtës së autorit direkt ose të ndërmjetësve.

23 Uarda Albunesa, *E drejta e autorit në shëipëri dhe në legjislacionin europian; përqasja mes tyre*, Doktoratura, Tiranë, 2014, fq.71.

24 Julien Hofmamn, *Introducing Copyright: A plain language guide to copyright in the 21st century,* Commonwealth of learning, Vancouver, 2009, fq.44-47.

25 Neni 46 i Marrëveshjes TRIPS.

26 Neni 61 i Marrëveshjes TRIPS.

III. Mbrojtja me mjete administrative e të drejtës së autorit

Mbrojtja e të drejtës së autorit në Shqipëri nëpërmjet rrugës administrative bëhet nëpërmjet masave doganore dhe nëpërmjet mbikëqyrjes në tregun e brendshëm.

a) Masat doganore dhe kontrolli në kufi:

Masat doganore njihen ndryshe dhe si masat në kufij për të mbrojtur të drejtat e pronësisë intelektuale. Këto masa kanë për qëllim parandalimin e shkeljeve të të drejtave të autorit duke ndalar kopjet e paligjshme të një vepre të së drejtës së autorit. Kjo mënyrë shihet si një mjet efektiv për të kundërshtuar shkeljet e së drejtës së autorit, pasi është më e lehtë që ti ndalosh këto kopje në kufij sesa kur vihen në qarkullimin tregtar.[27]

Kërkesa e mbajtësit të së drejtës së autorit ose e një të drejte të lidhur me të ose të një AAK-je, për raste të dyshimit të shkeljes së të drejtave në import, eksport ose kalim të paligjshëm të territorit doganor të Republikës së Shqipërisë bëhet në përputhje me legjislacionin doganor për mbrojtjen e të drejtave të pronësisë intelektuale.

b) Mbikëqyrja e tregut të brendshëm dhe kundravajtjet administrative:

Kundravajtjet administrative janë të parashikuara në pjesën e IX të ligjit nr.35/2016 "Për të drejtat e autorit dhe për të drejtat e tjera të lidhura me to". Për të mbikëqyrur ligjin për të drejtat e autorit dhe për të kontrolluar zbatimin e tij në tregun e brendshëm vepron inspektorati përgjegjës që mbulon fushën e mbikëqyrjes së tregut, pranë Ministrisë përgjegjëse për tregtinë në përputhje me ligjin për inspektimin. Ky inspektorat ngrihet dhe funksionon në bazë të VKM-së përkatëse[28]. Në përbërje të tij janë inspektorët, të cilët duhet që të kontrollojnë zbatimin e këtij ligji. Inspektorët vendosin ndaj kundërvajtësit dënimin kryesor me gjobë dhe dënimet plotësuese, kur gjatë inspektimit konstatojnë shkeljet, nën juridiksionin e të cilëve është kryer kundërvajtja administrative.[29]

Objekti i kontrollit të inspektorëve konsiston në *produktin fizik dhe/ose në kontrollin e lejes së lëshuar* nga mbajtësit e të drejtave ose agjencitë e licencuara të administrimit kolektiv, sipas parashikimeve të ligjit. Inspektorët mund që të bashkëpunojnë me autoritetet doganore e tatimore, Policinë

27 WIPO, *WIPO Intellectual Property Handbook*, Geneva, 2004, fq.216.

28 VKM Nr.36/2016 "Për krijimin, funksionimin dhe organizimin e Inspektoratit Shtetëror të Mbikëqyrjes së Tregut".

29 Uarda Albunesa, *E drejta e autorit në legjislacioni shqiptar dhe atë europian, përqasja mes tyre*, Doktoratura, Tiranë, 2014, fq.72.

e Shtetit dhe strukturat e krimit ekonomik, si edhe çdo institucion tjetër përgjegjës zbatues dhe mbikëqyrës për respektimin e të drejtave të autorit dhe të drejtave të lidhura apo mbajtësve të ligjshëm të tyre.[30]

Aktualisht në Shqipëri funksionon Inspektorati Shtetëror i Mbikëqyrjes së Tregut i cili është dhe garant për zbatimin e legjislacionit mbi të drejtat e autorit dhe të drejtat e tjera të lidhura me to. Inspektorati Shtetëror i Mbikëqyrjes së Tregut (ISHMT) është krijuar me VKM-në nr. 36, datë 20.01.2016 "Për krijimin , organizimin dhe funksionimin e Inspektoratit Shtetëror të Mbikëqyrjes së Tregut". ISHMT është institucion në varësi të Ministrisë së Financës dhe Ekonomisë dhe është përgjegjës për inspektimin në fushën e sigurisë së produkteve jo ushqimore për përdorim nga konsumatorët dhe fushën e pronësisë intelektuale. Ngritja e këtij inspektorati ishte nevojë e diktuar jo vetëm nga vetë zhvillimi ekonomik i vendit i parë në aspektin e rritjes së besimit të konsumatorit në treg e të konkurrencës së lirë, por edhe nga procesi integrimit të Shqipërisë në BE dhe përafrimin e legjislacionit të saj me acquis. Në dy raport progreset e Komisionit Europian të vitit 2015 dhe 2016 ngritja e ISHMT-së ka qenë një nga rekomandimet më të rëndësishme për Kapitullin 1 të lëvizjes së lirë të mallrave dhe një nga prioritetet për rregullimin dhe mbikëqyrjen e tregjeve në kapitullin Zhvillimi Ekonomik i Programit të Qeverisë Shqiptare 2013-2017.[31]

Janë një sërë kundravajtjesh administrative të cilat janë të parashikuara në nenin 179 pika 1 të ligjit nr.35/2016 që mbulojnë jo vetëm të drejtat pasurore por edhe ato vetjake jopasurore. Kundravajtjet administrative i referohen si të drejtave të autorit ashtu dhe të drejtave të tjera të lidhura me to, apo masave teknologjike për mbrojtjen e së drejtës së autorit.

Në rastet e kryerjes së kundravajtjes administrative është e rëndësishme të provohet se veprimet apo mosveprimet e palës së cilës i referohet shkelja e së drejtës së autorit të jetë kryer të jetë kryer me faj, duke treguar se cilat urdhërime ligjore janë shkelur.`[32]

Për këto kundravajtje administrative personi përgjegjës i personit juridik (administratori) dënohet me gjobë në shumën prej 100 000 deri në 500 000 lekësh. Nga ana tjetër nëse kundravajtja kryhet nga një person fizik[33], atëherë ai dënohet me gjobë në shumën prej 100 000 deri në 500 000 lekësh. Personi fizik, punonjës i çdo kategorie, ose çdo person tjetër i vetëpunësuar,

30 Neni 178 i ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

31 ishmt.gov.al/historiku/ aksesuar për herë të fundit më 21.05.2020.

32 Vendimi nr.603 datë 13.11.2018 i Gjykatës Administrative të Shkallës së Parë Gjirokastër.

33 Ne kuptim të personit fizik sipas legjislacionit tregtar në Shqipëri.

përkatësisht, dënohet me gjobë në shumën prej 50 000 deri 200 000 lekësh, respektivisht, ku kundërvajtja është kryer gjatë aktiviteteve të saj/të tij dhe që kishte dijeni apo ka pasur mundësinë për të marrë dijeni për të vërtetuar nëse ishte duke kryer një aktivitet të kundërligjshëm.[34] Kjo është një ndarje që është bërë në varësi të organizimit të subjektit kundërvajtës, ku parashikohet dhe një përgjegjësi më e madhe për personat juridikë dhe më e vogël për personat fizikë si dhe për personat e punësuar apo të vetëpunësuar.[35]

Kur konstatohet një shkelje e së drejtës së autorit nevojitet që për efekt provueshmërie në procesverbal të përshkruhen gjetjet e faktit duke përcaktuar çfarë produkti (vepre) është komunikuar në publik, shpërndarë, riprodhuar, si dhe kush është autori apo mbajtësi i së drejtës të cilit i janë cënuar të drejtat. Ky arsyetim është i rëndësishëm për të përcaktuar elementët objektivë të veprimeve apo mosveprimeve të cilat konsiderohen si kundravajtje administrative.[36]

Objektet dhe mjetet e përdorura për kryerjen e kundravajtjeve administrative të përmendura më sipër konfiskohen dhe shkatërrohen nga strukturat përkatëse, në përputhje me legjislacionin në fuqi për kundravajtjet administrative.[37] Ndaj personit që kryen kundravajtje administrative (person fizik apo juridik), gjatë ushtrimit të veprimtarisë së tij tregtare, mund që të merret masa e ndalimit të kryerjes së aktiviteteve të tij treegtare, për shkeljen e së drejtës së autorit apo të drejtave të tjera të lidhura me to, për një periudhë 1 vjeçare duke marrë parasysh edhe seriozitetin e shkeljeve dhe përsëritjen e këtyre shkeljeve nga ana e tyre.[38] Pra, kurdoherë nëse merret një masë e tillë ajo duhet që të jetë proporcionale.

Gjatë kryerjes së një procedure inspektimi, nevojitet që të kryhet një procedurë në përputhje me ligjin nr.10433 "Për inspektimin në Republikën e Shqipërisë", i ndryshuar, i cili është dhe ligji procedural i inspektimit, si dhe me ligjin nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to", që përbën ligjin material.[39]

Nëse këto kundravajtje administrative përsëriten, atëherë masa

34 Pika 2, 3 dhe 4 e nenit 179 të ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

35 Vendimi nr.2747 datë 13.07.2018 i Gjykatës Administrative të Shkallës së Parë Tiranë.

36 Vendimi nr.465 datë 04.12.2018 i Gjykatës Administrative të Shkallës së Parë Gjirokastër.

37 Neni 179 pika 5 i ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

38 Neni 179 pika 6 e ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

39 Vendimi nr.80-2018-2632, datë 03.07.2018 i Gjykatës Administrative të Shkallës së Parë Tiranë.

ndëshkimore maksimale e përcaktuar mësipër dyfishohet.[40] Të ardhurat që vijnë nga gjobat kalojnë në Buxhetin e Shtetit.[41] Inspektorët kanë të drejtë të kërkojnë ndihmën e Policisë së Shtetit, në rast se pengohen në ushtrimin e kompetencave të tyre ligjore, në përputhje me dispozitat e ligjit për inspektimin.[42]

Ankimi ndaj vendimeve të trupave inspektues, të përcaktuar në ligjin nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to", bëhet në përputhje me ligjin për inspektimin[43], ndërsa procedurat e konstatimit, shqyrtimit, vendosjes, ankimit dhe ekzekutimit të gjobave bëhen në përputhje me legjislacionin në fuqi për kundërvajtjet administrative. Pas përfundimit të procedurave të ankimit administrativ bëhet ankim në gjykatën administrative, brenda afateve dhe sipas procedurave të parashikuara në dispozitat e ligjit nr. 49/2012 "Për organizimin dhe funksionimin e gjykatave administrative dhe gjykimin e mosmarrëveshjeve administrative".

IV. Përfundime

E drejta e autorit është një tërësi të drejtash ligjore e cila merret me mbrojtjen e të drejtave të krijuesve mbi veprat letrare apo artistike. Qëllimi i së drejtës së autorit është të promovojë kulturën, artin dhe zhvillimin teknologjik e shkencor. Kjo bëhet duke shpërblyer autorët për krijimet e punimet e tyre, si dhe duke ruajtur një balancë ndërmjet autorëve, sipërmarrësve (botues, transmetues, prodhues fonogrami etj) dhe interesit publik. Të drejtat ekonomike të autorit e lejojnë atë që të përfitojë nga riprodhimi apo nga shfrytëzimi i veprës së tyre. Krijimet e autorit në të shumtën e legjislacioneve të shteteve të ndryshme njihen me emrin ***"vepër".***

Zbatimi i të drejtave të autorit nënkupton të gjitha ato masa që ndërmerren në rastet kur kemi shkelje apo cënim të së drejtës së autorit apo të drejtave të tjera të lidhura me to. Zbatimi i të drejtave të autorit ka pasur një evolucion galopant vitet e fundit për shkak të ndryshimeve teknologjike duke përfshirë këtu teknologjinë digjitale, e cila lejon që shumë vepra të transmetohen apo të kopjohen pa kurrëfarë kontrolli. Një tjetër arsye në lidhje me krijimin e

40 Neni 179 pika 10 e ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

41 Neni 170 pika 11 e ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

42 Neni 179 pika 7 e ligjit nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".

43 Aktualisht afati i ankimit ndaj një vendimi përfundimtar të inspektimit është 30 ditë nga marrja dijeni.

një sistemi të zbatimit të të drejtave të autorit është dhe fakti se këto mallra dhe shërbime të mbrojtura nga e drejta e autorit kanë një impakt ekonomik në tregun e brendshëm dhe atë ndërkombëtar.

Masat administrative luajnë një rol të rëndësishëm në ruajtjen e standarteve të tregtisë dhe rol ndihmës në ruajtjen dhe zbatimin e të drejtave të pronësisë intelektuale. Për shembull autoritetet doganore kryejnë veprimtarinë administrative në kufi për të parandaluar rastet e piraterisë së të drejtave të autorit. Me kërkesë të mbajtësit të së drejtës autoritetet administrative mund që të kryejnë ndalime të importeve të cilat shkelin të drejtat e autorit, apo në vendet ku kryhen inspektime të parandalojnë kryerjen e shkeljeve të të drejtave të autorit. Mbrojtja në nivel administrativ konsiderohet ndryshe edhe si një investim i shtetit për të mbrojtur krijimtarinë letrare, artistike dhe shkencore në vend.

V. Bibliografia

- Ligji nr.35/2016 "Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to".
- Marrëveshja "TRIPS" (Mbi disa aspekte të tregtisë së lirë dhe pronësisë intelektuale).
- VKM Nr.36/2016 "Për krijimin, funksionimin dhe organizimin e Inspektoratit Shtetëror të Mbikëqyrjes së Tregut".
- Vendimi nr.603 datë 13.11.2018 i Gjykatës Administrative të Shkallës së Parë Gjirokastër.
- Vendimi nr.2747 datë 13.07.2018 i Gjykatës Administrative të Shkallës së Parë Tiranë.
- Vendimi nr.465 datë 04.12.2018 i Gjykatës Administrative të Shkallës së Parë Gjirokastër.
- Vendimi nr.80-2018-2632, datë 03.07.2018 i Gjykatës Administrative të Shkallës së Parë Tiranë.
- Drejtoria për të Drejtën e Autorit, Të kuptojmë të drejtën e autorit dhe të drejtat e tjera të lidhura me të, Broshurë.
- Fatos Dega, Pronësia Intelektuale, Botimi i IV, Morava, Tiranë, 2014.
- Tate Legal, A brief Guide to Copyright, August, 2016.
- WIPO, Advanced Course on Copyright and Related Rights, Module

I: The Concept of Copyright, the Historical Background and the International Framework, Geneva, 2019.

- Paul Torremans, Holyak & Torremans Intellectual Property Law, 7th Edition, Oxford University Press, UK, 2013.
- Robert A. Gorman, Copyright Law, Federal Judicial Center, 2006.
- The Institute of Company Secretaries of India, Intellectual Property Rights-Law and Practice, Study Material, New Dehli.
- Aaron Schwabach, Intellectual Property: A Reference Handbook, ABC-CLIO, England, 2007.
- WIPO, WIPO Intellectual Property Handbook, Geneva, 2004.
- Jennifer Davis, Intellectual Property Law, 4th Edition, Oxford University Press, Hampshire, 2012.
- Uarda Albunesa, E drejta e autorit në shëipëri dhe në legjislacionin europian; përqasja mes tyre, Doktoratura, Tiranë, 2014.
- Julien Hofmamn, Introducing Copyright: A plain language guide to copyright in the 21st century, Commonwealth of learning, Vancouver, 2009.

WIPO, *WIPO Intellectual Property Handbook: Policy, Law and Use*, Second Edition, 2008

ishmt.gov.al/historiku/

PREVENTION AND DETECTION OF CRIMES BY TECHNOLOGICAL MEANS

MSC. ARBER TOÇI
DR. IVROKAJ LL.M

Abstract

Organized crime and corruption are two phenomena which are closely related to each other, as they have a single purpose, the one of creating and illegally obtaining wealth, violating the general interest of society in a certain place, at a certain time.

Technology in itself refers to material objects that are created and used by man in order to achieve the most satisfactory results. Through the use of technology, it is noë possible not only to achieve good results in crime prevention but also to discover the perpetrators of criminal offenses, capture them and establish irrefutable facts and evidence before the responsibility for the crime committed.

Through this paper we will try to point out what are the positive sides of the use of technology in crime prevention and investigation and what needs to be done more to be more efficient in the use of these technological tools.

The use of technology has become by far one of the key ëeapons in preventing organized crime and corruption. Knowledge of technological tools and their use has become a key factor ëhich makes possible the prevention and detection of crimes, not only the one which are based on technology for their realization, but criminality in general

This article will explore different technological improvements that have a significant role in crime prevention for organized crime and corruption.

Keywords: Organized crime, corruption, technology, investigation, prevention

PARANDALIMI DHE ZBULIMI I KRIMEVE ME MJETE TEKNOLOGJIKE

ABSTRAKTI

Krimi i organizuar dhe korrupsioni janë dy dukuri të lidhura ngushtë me njëra-tjetrën, pasi kanë një qëllim të vetëm, atë të krijimit dhe marrjes së paligjshme të pasurisë, cenimit të interesit të përgjithshëm të shoqërisë në një vend të caktuar, në një kohë të caktuar.

Teknologjia në vetvete i referohet objekteve materiale që krijohen dhe përdoren nga njeriu për të arritur rezultatet më të kënaqshme. Nëpërmjet përdorimit të teknologjisë tashmë mund të arrihet jo vetëm rezultate të mira në parandalimin e krimit, por edhe zbulimi i autorëve të veprave penale, kapja e tyre dhe vërtetimi i fakteve dhe provave të pakundërshtueshme përpara përgjegjësisë për krimin e kryer.

Nëpërmjet këtij punimi do të përpiqemi të vëmë në dukje se cilat janë anët pozitive të përdorimit të teknologjisë në parandalimin dhe hetimin e krimit dhe çfarë duhet bërë më shumë për të qenë më efikas në përdorimin e këtyre mjeteve teknologjike.

Përdorimi i teknologjisë është bërë një nga armët kryesore në parandalimin e krimit të organizuar dhe korrupsionit. Njohja e mjeteve teknologjike dhe përdorimi i tyre është bërë një faktor kyç që bën të mundur parandalimin dhe zbulimin e krimeve, jo vetëm të atyre që bazohen në teknologji për realizimin e tyre, por kriminalitetit në përgjithësi.

Ky artikull do të shqyrtojë përmirësime të ndryshme teknologjike që kanë një rol të rëndësishëm në parandalimin e krimit për krimin e organizuar dhe korrupsionin.

Fjalët kyçe: Krimi i organizuar, korrupsioni, teknologjia, hetimi, parandalimi

HYRJE

Parandalimi i krimit dhe zbulimi i tij, tradicionalisht përfshijnë ndër të tjera metoda jo-shkencore si patrulla në këmbë, policimi në komunitet, duke u betuar para zotit nëpërmjet përdorimit të librave të shenjtë (Kur'anit dhe Biblës), betimi para autoritetit publik, dënimi me burgim dhe frika nga izolimi etj.

Rrezikshmëria që paraqet krimi si një fenomen njerëzor përgjithësisht në botë, kanë bërë të nevojshme nevojën për të parë përtej metodat konvencionale ose mjetet tradicionale të parandalimin dhe zbulimin e tij.

Inovacioni teknologjik ishte forca lëvizëse që çoi në reformën e strategjive të parandalimit të krimit dhe kontrollit të krimit, si nga qytetarët individualë dhe grupet e interesuara, ashtu edhe nga agjencitë ligjzbatuese.

Teknologjia është identifikuar si instrument për parandalimin dhe zbulimin e krimit veçanërisht në vendet në zhvillim. Teknologjia brenda konteksti i këtij punimi përfshin mjete, procese dhe teknikat të cilat ndihmojnë organet ligjzbatuese të minimizojnë sa më shumë pasojat që sjell krimi në shoqëri. Nga ana tjeër disponueshmëria e shpejtë e teknologjisë së re në botën e krimit jo vetëm që u ka dhënë organeve të zbatimit të ligjit një gamë më të madhe mjetesh dhe metodash të reja për t'i ndihmuar ata në kohën e tanishme të drejtësisë penale por u ka vështirësuar atyre zbulimin e autorëve të krimit.

Ekzistojnë dy lloje të përgjithshme teknologjike të cilat që mund të identifikohen si: teknologjitë e bazuara në informacion (të cilave do t'i referohemi si teknologji e butë) dhe teknologjitë e bazuara në material (të cilave do t'u referohemi si teknologji të vështira).

Të dyja llojet e inovacionit teknologjik kanë qenë të lidhura me "Ndryshime dramatike në organizimin e policisë" veçanërisht në fillim të shekullit të kaluar, ndërkohë që lidhje të ngjashme mund t'i ofrohen krimit më të përgjithshëm strategjitë parandaluese të përdorura nga individë dhe grupe banorësh. Sipas një rishikimi të fundit të teknologjisë policore nga Harris[1], teknologjia e parë revolucioni në SHBA që ndryshoi mënyrën e organizimit dhe mënyrën e organizimit të policisë ato operuan të përqendruara rreth tre inovacioneve teknologjike që u përfshinë në polici: telefoni, radio me dy drejtime (marrëse-dhënëse) dhe automobili.

1 HARRIS, C. (2007) "Police and Soft Technology:

I. TEKNOLOGJIA BIOMETRIKE

1. Daktiloskopia (gjurmet e vijave papilare)

Marrja e gjurmëve papilare nga një skenë krimi është një metodë e rëndësishme e shkencës mjeko-ligjore. Daktiloskopimi, përkatësisht marrja e shenjave të vijave papilare të personit zbatohet në mënyrë që të mund të bëhet krahasimi i atyre personave që kanë mundur t'i lënë gjurmët e vijave papilare në vendin e ngjarjes, në sende etj. Daktiloskopimi bëhet në kuadër të të ashtuquajturit përpunimit sinjalitik të personit. Për nevojat e daktiloskopimit nevojiten mjete të caktuara:

- *Pllaka e porelonit,*
- *Mbajtësja e kartonit,*
- *Kartonat përkatës daktiloskopik,*
- *Mjetet për pastrim.*
- *Duhet thënë se përveç këtyre mjeteve për lloje më të ndërlikuara të daktiloskopimit përdoren edhe ngjyra e zezë e shtypit ose ngjyra daktiloskopike dhe, pllaka e lëmuar prej xhami me dimensione 12 x 30.* [2]

Nga këndvështrimi i shkencës së kriminalistikës gjurmët e vijave papilare konsistojnë në disa drejtime, si:

- *Së pari,* për të identifikuar personin që ka kryer vepren penale mbi bazën e gjurmëve papilare të lëna në vendin e ngjarjes;
- *Së dyti,* për të vërtetuar që më shumë se një vepër penale, ku janë zbuluar gjurmë papilare, janë kryer nga i njëjti person;
- *Së treti,* për të identifikuar një kufomë të panjohur, të skeduar me kartelë daktiloskopike si person me precedent penal, mbi bazën e vijave papilare;
- *Së katërti,* për të zbuluar falsitetin e një dokumenti ideintiteti, të një personi, si një pasportë, letërnjoftim etj., në të cilin si element sigurie, përpos të tjerash, ka dhe gjurmë papilare.
- *Së pesti,* me zvillimin e teknologjisë vijat papilare përdoren edhe në fushën e sigurisë, si kod për të hapur objekte të ndryshmë, si dyer telefona etj..

2 Veliqoti L. "Kriminalistika",Vëllimi I "Geer" Tiranë 2015.

2. ADN (acid deoksiribonukleik)

Prezantimi i analizës së ADN-së ishte ndoshta përparimi më i madh në drejtim të analizimit të provave. AND-ja është molekula biologjike më e famshme, të gjitha format e jetës në tokë e kanë të pranishme këtë lloj molekule. Një molekulë e cila përmban kodin gjenetik unik të secilit person quhet ADN. Mban udhëzimet për ndërtimin e proteinave të cilat janë thelbësore për funksionomin e trupit. ADN mbart udhëzimet për zhvillimin, rritjen, riprodhimin dhe funksionimin e gjithë jetës. AND-ja është molekulë të cilës udhëzimet e saj kalohen nga prindërit tek fëmija. Saktësisht gjysma e AND-së ka origjinën nga babai dhe gjysma nga nëna.

Në kuadër të analizave të ADN-së kryhen këto analiza:

- *Analizat e ADN-së nga pështyma,*
- *Analizat e ADN-së nga gjaku,*
- *Analizat e ADN-së nga qimet dhe indet*
- *Analizat e ADN-së nga sperma,*
- *Analizat e ADN-së nga eshtrat dhe dhëmbët*
- *Analizat e ADN-së nga prekja apo kontakti (djersa dhe qelizat epiteliale)*

II. TEKNOLOGJIA E KOMUNIKACIONIT DHE AUDIO-VIZIVE

1. Përgjimet elektronike

Përgjimi elektronik nënkupton përgjimin e komunikimeve të çdo lloji të një personi ose numri telefonik, nëpërmjet telefonit, faksit, kompjuterit ose ndonjë mjeti tjetër; përgjimin e fshehtë të bisedave në mjedise private, nëpërmjet mjeteve teknike; përgjimin audio dhe video në mjedise private e publike; regjistrimin e thirrjeve telefonike hyrëse dhe dalëse telefonike, si dhe përdorimin e pajisjeve gjurmuese për të zbuluar vendndodhjen. Përgjimet elektronike mund të urdhërohen ndaj:

- *të dyshuarit për kryerjen e një vepre penale;*
- *personit që mendohet se komunikon me të dyshuarin;*

- *personit që merr pjesë në transaksione me të dyshuarin;*
- *personit, vëzhgimi i të cilit mund të çojë në zbulimin e vendndodhjes apo identitetit të të dyshuarit*[3].

2. Gjurmimi

Pajisjet gjurmuese janë pajisje elektronike që tregojnë vendndodhjen ose që ndjekin lëvizjen e një personi ose sendi (p.sh: një pako ose një automjet). Sipas ligjit, përdorimi i këtyre pajisjeve lejohet me autorizim të prokurorit.

Aktualisht, organet e zbatimit të ligjit disponojnë disa lloje pajisjesh gjurmuese. Pajisjet më të reja kanë të bëjnë me teknologjinë GPS (Sistemi Global i Pozicionimit). GPS u zhvillua në vitet 1970 nga Departamenti Amerikan i Mbrojtjes në mënyrë që njësitë ushtarake të mund të njohin gjithmonë vendin e saktë dhe vendndodhjen e njësive të tjera. Sistemi Global i Pozicionimit (GPS) i ndihmoi Shtetet e Bashkuara të fitonin luftën në Gjirin Persik më 1991. Gjatë Operacionit Stuhia e Desertit , automjetet ushtarake u mbështetën në sistem për të lundruar nëpër shkretëtirë shterpë gjatë natës.

Kjo teknologji, e zhvilluar fillimisht nga ushtria amerikane, mbështetet në një konstelacion prej 27 satelitësh që rrotullohen rreth Tokës. Orbitat e tyre janë pozicionuar në një mënyrë të tillë që, në çdo moment, nga çdo pikë në Tokë, janë të dukshëm të paktën 4 satelitë. Marrësi GPS lokalizon të paktën 4 prej këtyre satelitëve, gjen distancën e tij nga secili përmes valëve të radios që satelitët lëshojnë, dhe nëpërmjet një procesi që bazohet në parimin matematikor të trefaqëzimit arrin të saktësojë vendndodhjen e tij. Disa telefona celularë janë të pajisur me teknologji GPS, e cila lejon përdoruesin e telefonit që të gjejë vendndodhjen e tij, por, nga ana tjetër, lejon edhe hetuesit ta gjejnë këtë vendndodhje, duke i drejtuar një kërkesë ofruesit të shërbimit të telefonisë celulare. Ofruesi i shërbimit ka, gjithashtu, mundësinë teknike të japë edhe informacionin historik, pra vendndodhjet e mëparshme të telefonit. Disa marrës GPS kanë edhe kapacitetin të regjistrojnë në audio. Para se hetuesit të përdorin një pajisje të tillë në një vend privat, ata duhet të marrin miratimin e gjykatës.[4]

3 Neni 221/3 i Kodit të Procedurës Penale

4 https://www.gps.gov/

3. Kulla e telefonisë celulare – Trekëndëzimi

Një metodë tjetër është ajo që njihet si "Trekëndëzimi i kullave të telefonisë celulare" (Cell Toëer Triangulation), që do të thotë se kullat e telefonisë celulare, të cilat marrin sinjalin e telefonit mund të përdoren për të llogaritur vendndodhjen gjeofizike të tij. Në rastet më të mira sinjali i një telefoni celular mund të kapet nga tre ose më shumë kulla të telefonisë celulare, duke bërë të mundur që të funksionojë "trekëndëzimi". Nga këndvështrimi gjeometrik/matematik, nëse njihet distanca e një sendi nga tre pika të veçanta, mund të llogaritet edhe vendndodhja e tij e përafërt, në raport me vendndodhjen e tre pikave të referimit. (kullave).

Kjo llogaritje gjeometrike aplikohet në rastin e telefonave celularë, meqënëse dimë vendndodhjen e antenave të telefonisë celulare, të cilat marrin sinjalin e telefonit, dhe mund të llogarisim distancën e telefonit nga secila prej tyre, bazuar në kohën që kalon mes pingut që dërgon antena dhe pingut të përgjigjes nga telefoni. Edhe në këtë rast hetuesit mund ta gjejnë vendndodhjen, duke i drejtuar një kërkesë ofruesit të shërbimit të telefonisë celulare. Ofruesi i shërbimit ka, gjithashtu, mundësinë teknike të japë edhe informacionin historik, pra vendndodhjet e mëparshme të telefonit.[5]

III. TEKNOLOGJIA DIXHITALE

1. Provat elektronike

Prova dixhitale është informacion ose e dhënë që ka vlerë për hetimin, e cila ruhet, merret ose transmetohet nga një pasjisje elektronike. Kjo provë merret kur të dhënat ose pajisjet elektronike sekuestrohen për kqyrje.

Ndërsa ruajtja dixhitale e informacionit përhapet përherë e më shumë, kriminalistika dixhitale, marrja dhe analizimi i informacionit dixhital, bëhet përherë e më e rëndësishme për prokurorët dhe policinë gjyqësore. Mbledhja e këtyre të dhënave dhe prezantimi i tyre në gjyq duhet të bëhet sipas rregullave të përgjithshme të mbledhjes së provave. Sikurse edhe prova të tjera materiale, p.sh: kufoma, dokumentet dhe pajisjet e ruajtjes së informacionit dixhital duhet të ruhen me kujdes, për të shmangur pretendime se provat janë manipuluar apo ndotur.

5 https://www.iiiweb.net/forensic-services/cell-phone-tower-triangulation/

Nga çdo pajisje e ruajtjes së informacionit dixhital mund të nxirren prova thelbësore. P.sh: nga një telefon celular mund të nxirren numra të fshirë telefoni që tregojnë se një person njeh një tjetër, megjithëse e mohon këtë fakt; takimet e regjistruara në një kompjuter dore mund të përcaktojnë një kronologji ngjarjesh. Madje, edhe programet televizive të regjistruar në një video-regjistrues dixhital mund të konfi rmojnë ose të hedhin poshtë një alibi, duke treguar se kur ka fi lluar ose është ndërprerë regjistrimi. Teorikisht, të gjitha këto prova janë të rekuperueshme. Më poshtë do të bëjmë një përmbledhje të llojeve të provave që mund të nxirren nga sisteme të tilla, që shërben si udhëzim në lidhje me marrjen dhe sigurimin e këtyre provave.

Parimet e përgjithshme kriminalistike dhe procedurale duhet të zbatohen edhe për provat dixhitale të cilat janë:

- Procesi i mbledhjes, sigurimit dhe transportimit të provave dixhitale nuk duhet ta ndryshojë provën;
- Provat dixhitale duhet të analizohen vetëm nga persona të trajnuar në mënyrë të posaçme për atë qëllim;
- Çdo veprim i kryer gjatë sekuestrimit, transportimit dhe ruaj tjes së provave dixhitale duhet të dokumentohet plotësisht, të ruhet dhe të jetë i disponueshëm për shqyrtim. Të dhënat kompjuterike dhe provat e tjera dixhitale janë delikate, prandaj hetuesit e patrajnuar dhe pa aftësitë e nevojshme nuk duhet të kqyrin përmbajtjen e tyre ose të përpiqen të rekuperojnë informacion.

Prova dixhitale ka disa karakteristika të cilat mund të ndikojnë negativisht nëse ato nuk trajtohen me shpejtësi dhe efikasitet:

- Është e fshehur, që do të thotë se, zakonisht, vlera e saj si provë nuk është e dukshme për syrin e lirë, por nevojiten procese të veçanta ose kqyrje kriminalistike që të "zbulojnë" natyrën e saj (njëlloj si gjurmët e gishtërinjve ose të ADN-ja);
- Kapërcen shpejt dhe lehtësisht kufijtë jurisdiksionalë;
- Mund të ndryshohet, dëmtohet ose shkatërrohet lehtësisht;
- Mund të mos i qëndrojë kohës, pra duhet të trajtohet me shpejtësi. Hetuesit duhet të mbajnë parasysh se provat dixhitale mund të përmbajnë edhe prova materiale, p.sh: ADN, gjurmë gishtash apo njolla gjaku. Provat materiale duhet të ruhen, në mënyrë që të kryhet ekzaminimi i duhur.

2. Sistemet kompjuterike

Sistemet kompjuterike përmbajnë pajisje kujtese (hardëare) dhe programe (softëare) që përpunojnë të dhëna.

Një sistem kompjuterik mund të përfshijë:

- *Një kasë metalike që përmban qarqe, mikroproçesorë, pajisje kujtese (hard drive) dhe mjete ndërlidhëse;*
- *një monitor ose pajisje të shfaqjes së videos;*
- *një tastierë;*
- *një mi;*
- *përbërës periferikë ose pajisje kujtese dhe përbërës të tjerë të jashtëm.*

Sistemet kompjuterike janë të formave të ndryshme, si: kompjuter prehri (laptop), kompjuter tavoline (desktop), njësi qëndrore kompjuteri (toëer), sisteme të montuara (rack mounted), minikompjuter dhe kompjutera të mëdhenj (mainframe).

Përbërës të tjerë dhe pajisje periferike mund të jenë modemi, ruterat, printerat, skanerat, pajisjet për karikim baterish dhe pajisjet lidhëse.

Një sistem kompjuterik dhe përbërësit e tij mund të sjellin shumë prova vlefshme në një hetim. Pajisjet e kujtesës, programet, dokumentet, fotografi të, skedat me imazhe, mesazhet e postës elektronike me dokumentet bashkëlidhur, bazat e të dhënave, informacion fi nanciar, historia e faqeve të vizituara në internet, listat e çatit, listat e miqve, kalendarët e veprimtarive, të dhëna të ruajtura në pajisje të jashtme dhe çdo informacion tjetër identifi kues që merret nga sistemi kompjuterik dhe përbërësit e tij janë të gjitha prova të mundshme.

3. Pajisjet e ruajtjes së informacionit

Pajisjet e ruajtjes së informacionit ndryshojnë nga përmasat dhe nga mënyra e ruajtjes së informacionit. Por, pavarësisht kësaj këto pajisje mund të përmbajnë informacion që është i vlefshëm për hetimin ose ndjekjen penale.

Llojet e pajisjeve të ruajtjes së informacionit:

- Pajisjet e kujtesës (hard drive) janë pajisje të ruajtjes së informacionit

që ndodhen brenda kasës së kompjuterit dhe përbëhen nga një bord qarqesh të jashtëm, lidhje ushqimi dhe transmetimi të jashtme, dhe elementë të brendshëm prej xhami, qeramike ose metali të ngarkuar me magneticitet, të cilët ruajnë informacionin. Pajisja e kujtesës është truri i kompjuterit dhe përmban të gjithë programet e nevojshme për funksionimin e kompjuterit. Ajo ruan funksionet e kryera ose të ruajtura në kompjuter, p.sh: dokumentet, mesazhet e hapura të postës elektronike dhe dokumentet bashkëlidhur në to. Hetuesit mund të gjejnë në vendngjarje edhe pajisje kujtese që nuk janë të lidhura ose të instaluara në një kompjuter, por edhe këto mund të përmbajnë prova të vlefshme.

- Pajisjet e jashtme të kujtesës (hard drive të jashtëm) mund të instalohen edhe në një kasë të jashtme. Ata mund të rrisin kapacitetin e kompjuterit për të ruajtur të dhëna, por, njëkohësisht janë të lëvizshëm. Përgjithësisht, këto pajisje kanë nevojë për një burim ushqimi, si dhe një lidhje USB, FireWire, Ethernet ose pa kabëll me një sistem kompjuteri.
- Pajisjet e lëvizshme të ruajtjes janë lloje të ndryshme disqesh dhe, zakonisht, përdoren për të ruajtur, arkivuar, transferuar dhe transportuar të dhëna dhe informacione të tjera. Këto pajisje ndihmojnë përdoruesit për të shkëmbyer të dhëna, informacion dhe aplikime mes kompjuterave dhe pajisjeve të ndryshme. Këto mjete përfshijnë disketat (Floppy Disk), disketat e komprensimit (Zip Disk), CD-të (Compact Disc) dhe DVD-të (Digital Versatile Disc).
- Flash drive janë pajisje të vogla, të lehta, të lëvizshme me lidhje USB. Këto pajisje janë të lehta për t'u fshehur dhe për t'u transportuar. Ato prodhohen në formë ore, thike xhepi apo forma të tjera të pajisjeve të përdorimit të përditshëm.
- Kartat e kujtesës (Memory Card) janë pajisje të vogla të ruajtjes së të dhënave që përdoren zakonisht me aparatet fotografi kë dixhitalë, kompjutera, telefona celularë, axhenda dixhitale (PDA), pajisjet e lojërave elektronike dhe pajisje të tjera kompjuterike që mund të mbahen në dorë. Pajisjet e ruajtjes së informacionit mund të përmbajnë fotografi , skeda me imazhe, mesazhe të postës elektronike me dokumente bashkëlidhur, baza të dhënash, informacion fi nanciar, historinë e faqeve të vizituara në internet, lista të çatit, lista të miqve, kale ndarë veprimtarish, të cilët mund të përdoren si prova. [6]

6 Jerome H. Saltzer, M. Frans Kaashoek Instituti për Teknologji i Masaçusetsit – MIT, SHBA

4. Pajisjet kompjuterike të dorës

Këto janë pajisje të lëvizshme të ruajtjes së të dhënave që përdoren për komunikim, fotografi dixhitale, sisteme navigimi, zbavitje, ruajtje të dhënash dhe menaxhim të të dhënave personale. Pajisjet kompjuterike të dorës, si: telefonat celularë, axhendat dixhitale (PDA), pajisjet multimediale dixhitale (audio dhe video), pager-at, aparatet fotografi kë dixhitalë dhe marrësit GPS mund të përmbajnë programe, aplikime, dokumente, mesazhe të postës elektronike, histori të kërkimit në internet, listë çati, lista miqsh, fotografi , skeda imazhesh, baza të dhënash, të dhëna fi nanciare, të cilat mund të shërbejnë si prova në një çështje penale.

5. Pajisjet periferike

Pajisjet periferike lidhen me një kompjuter ose një sistem kompjuterik, për të përmirësuar aksesin e përdoruesit dhe për të zgjeruar funksionet e kompjuterit. Të tilla janë tastiera, miu, mikrofonat, portat USB dhe FireËire, lexuesit e kartave të memories, pajisjet VoIP dhe kamerat e rrjetit. Vetë pajisjet dhe funksionet që ato kryejnë ose lehtësojnë janë prova të mundshme. Informacioni i ruajtur në pajisje, i cili tregon përdorimin e saj, është gjithashtu provë, p.sh: numra hyrës dhe dalës telefonash dhe faksesh, dokumente të skanuar, faksuar ose printuar së fundmi, etj. Këto pajisje mund të jenë edhe burim i gjurmëve të gishtave, ADN-së dhe identifi kuesve të tjerë.

6. Burime të tjera të provave dixhitale

Hetuesit duhet të jenë të informuar dhe të vlerësojnë si prova edhe sende të tjera të ndodhur në vendngjarje, si: çdo pajisje elektronike, program, pajisje kujtese apo të ndonjë lloji tjetër dhe çdo teknologji që mund të funksionojë në mënyrë të pavarur ose të lidhet me sisteme kompjuterike. Këto pajisje mund të përdoren për t'i dhënë përdoruesit më shumë akses dhe mund të zgjerojnë funksionet e sistemit kompjuterik ose pajisjeve të tjera. Të tilla pajisje mund të jenë: kasetat e ruajtjes së të dhënave, pajisjet e përgjimit, aparate fotografi ke dixhitale, video-kamerat, video regjistratorët dixhitalë, audio regjistruesit dixhi talë, pajisjet e lojërave elektronike, pajisjet ndihmëse të çatit, tastierat, minjtë, çelësat për shkëmbimin e videos (KM), lexuesit e kartave SIM, GPS, marrës GPS dhe materiale shpjeguese që lidhen me to.

7. Rrjetet kompjuterike

Një rrjet kompjuterik konsiston në dy ose më shumë kompjutera, të lidhur

me kabllo të dhënash ose lidhje pa kabllo (ëireless), që shkëmbejnë ose kanë aftësi të shkëmbejnë mjete dhe të dhëna. Shpesh, një rrjet kompjuterik përfshin printera, pajisje të tjera periferike, pajisje për drejtimin e të dhënave, si: porta, çelësa dhe rutera. Rrjeti kompjuterik mund të përfshijë një server në distancë, pra një kompjuter që nuk është i lidhur me tastierën e përdoruesit, por mbi të cilin përdoruesi ushtron kontroll, pavarësisht nëse është në të njëjtën dhomë, në një pjesë tjetër të ndërtesës apo në një qytet a shtet tjetër. Serveri në distancë mund të shërbejë si pajisja kryesore e ruajtjes së informacionit ose si pajisja rezervë për funksionet që kryhen në kompjuterat e përdoruesve. Kompjuterat në rrjet dhe vetë pajisjet e lidhura në to mund të jenë prova të dobishme për hetimin penal.

Të dhënat që ata përmbajnë mund të jenë prova të vlefshme: programet, mesazhet e postës elektronike, historia e faqeve të vizituara në internet, listat e çatit, listat e miqve, skedat me imazhe, bazat e të dhënave, të dhënat fi nanciare, kalendarët e veprimtarive dhe të dhëna të ruajtura në pajisje të jashtme. Funksionet e pajisjeve, aftësitë e tyre dhe çdo informacion identifi kues që ka të bëjë me sistemin, duke përfshirë adresat IP dhe LAN të kompjuterave dhe pajisjeve; parametrat e transmetimit dhe kartat e medias (MAC), si dhe adresat e kartave të ndërfaqes së rrjetit (NIC) mund të jenë të gjitha të dobishme si prova.

Marrja e provave dixitale gjatë kontrollit Provat dixhitale në kompjutera ose në pajisje të tjera elektronike mund të ndryshohen, fshihen ose shkatërrohen lehtësisht. Këto prova duhet të merren e analizohen nga persona që janë trajnuar për marrjen e provave elektronike. Hetuesi i parë që bie në kontakt me vendin që kontrollohet duhet të sigurojë që të mos ndryshojë gjendja e pajisjeve elektronike. Kjo do të thotë p.sh: që nuk duhet të fi ket një kompjuter që gjendet në punë dhe që nuk duhet të ndizet një kompjuter ose pajisje elektronike që gjendet i fi kur. Disa pjesë të pajisjeve, si: tastiera, miu, mjetet e lëvizshme (fl ash drive), dhe sende të tjera mund të përmbajnë prova të fjetura (gjurmë gishtash, ADN) ose prova të tjera fi zike që duhet të ruhen. Hetuesit e parë që shkojnë në vendin e kontrollit duhet të marrin masat e duhura për të siguruar se provat fi zike nuk dëmtohen gjatë dokumentimit.

Hetuesi duhet të jetë i vëmendshëm ndaj mjedisit të vendit të kontrollit. Ai duhet të kërkojë për copa letre që mund të përmbajnë fjalëkalime, shënime me shkrim dore, blloqe me fl etë të pashkruara, në të cilët mund të gjenden shenjat e asaj që mund të jetë shkruar në faqet e grisura, manuale të programeve ose të pajisjeve kompjuterike, kalendarë, literaturë, tekste ose grafi ka të printuara nga kompjuteri që mund të japin informacione që kanë

të bëjnë me hetimin. Edhe këto lloje provash duhet të dokumentohen dhe të ruhen në përputhje me ligjin dhe aktet nënligjore.

8. Ekzaminimi kriminalistik

Ekzaminimi i kompjuterave dhe mjeteve të tjera elektronike të ruajtjes së informacionit duhet të bëhet vetëm nga persona me njohuri të thella të kriminalistikës kompjuterike. Megjithatë, hetuesit mund të ndihmojnë në procesin e ekzaminimit duke informuar specialistin kriminalistik në lidhje me llojin dhe natyrën e informacionit që po kërkojnë. Për këtë arsye, kur është e mundur, ata duhet t'i japin specialistit informacionin e mëposhtëm:

- një përmbledhje të çështjes;
- fjalëkalime të njohura të pajisjeve dixhitale të sekuestruara;
- raporte dhe dokumente paraprake;
- lista me fjalë kyçe;
- një pikën kontakti në grupin hetimor.

9. Provat dixhitale dhe krimet financiare e korrupsioni

Kqyrja e pajisjeve elektronike mund të urdhërohet nga prokurori, nëse kjo është e nevojshme për zbulimin e gjurmëve apo pasojave të tjera materiale të veprës penale7

Lloji i provave që mund të gjenden varet nga faktet e çështjes konkrete. Më poshtë jepet një listë jo shteruese e provave, të cilat mund të gjenden në pajisjet elektronike dhe mund të jenë me vlerë në rastet e krimit fi nanciar dhe korrupsionit. Përveç provave të rifi tuara nga pajisja elektronike, hetuesi duhet të hetojë edhe lidhjen mes pajisjeve dhe personave të caktuar, si përdorues të tyre, përmes marrjes së gjurmëve të gishtave, ADN-së, etj. Në një rast të tillë analizat jo shkatërruese për këto gjurmë duhet të kryhen me kujdes para se pajisjet të dorëzohen për kqyrjen e brendshme kriminalistike. Të gjitha proceset shkatërruese që kanë të bëjnë me marrjen ose analizimin e provave të fshehura, biologjike e mikrogjurmëve dhe provave të tjera duhet të shtyhen derisa të merren provat dixhitale për kqyrje e analizim.

- **mesazhe të postës elektronike:**

❖ komunikime që lidhen haptazi me veprën penale;

7 Neni 198 i Kodit të Procedurws Penale

- ❖ komunikime që përcaktojnë lidhjen/marrëdhënien me bashkëpunëtorë të mundshëm ose të dyshuar të tjerë;
- ❖ komunikime që tregojnë lidhjet e personave të dyshuar ose familjarëve të tyre me institucione financiare, investime dhe blerje duke dhënë kështu pista për hetime të mëtejshme;
- ❖ komunikime që tregojnë sjellje të tjera kriminale, sjellje imorale ose të dyshimta;

• dokumente dhe skeda:

- ❖ projekte letrash, memosh, kontratash, etj, që kanë lidhje me veprën penale. Kjo është veçanërisht me vlera kur kopjet fizike të këtyre dokumenteve janë gjetur diku tjetër dhe është e rëndësishme që të bëhet lidhja e personit nën hetim me përgatitjen e këtyre dokumenteve;
- ❖ drafte letrash, memosh, kontratash, etj, të cilat nuk janë haptazi të lidhura me veprën penale, por përcaktojnë marrëdhënien e personit nën hetim me bashkëpunëtorë të tjerë të mundshëm ose me prona, investime e blerje të caktuara; o lista kontratash dhe skeda adresash;
- ❖ kalendarë dhe axhenda personale; o lista me emra përdoruesish dhe fjalëkalime për faqe interneti, institucione bankare dhe karta krediti, etj;

• të dhëna financiare:

- ❖ të dhëna fi nanciare nga programe si QuickBooks, Quicken, Microsoft, etj; o grafi ka, përmbledhje, tabela dhe baza të dhënash që japin hollësi për të kaluarën fi nanciare apo blerjet e personit nën hetim;
- ❖ deklarata apo dokumente të tjerë tatimorë; o të dhënat për kartat e kreditit;

• foto dhe video:

- ❖ mund të përshkruajnë marrëdhënien e personit me bashkëpunëtorë ose të dyshuar të tjerë;
- ❖ mund të përshkruajnë ose të konfi rmojnë marrëdhënien e personit nën hetim me prona e asete të caktuara (fotografi në makinën së tij Ferrari);
- ❖ mund të konfi rmojnë ose të japin pista të reja në lidhje me shpenzime, si udhëtimet, bizhuteritë, etj; o mund të përshkruajnë sjellje të paligjshme, imorale ose të dyshimta;

• veprimtaria në internet:

- ❖ faqe interneti të institucioneve bankare, agjentëve financiarë apo institucioneve të tjera fi nanciare, të cilat mund të japin pista për llogari apo asete;
- ❖ faqe të lidhura me udhëtime dhe shitje/ankande online, të cilat mund të japin pista në lidhje me udhëtime dhe blerje të kryera; o dhomat e çatit të internet, rrjetet sociale (Facebook, etj), të cilat mund të japin pista të mëtejshme ose prova;
- ❖ faqe interneti pornografi ke ose për njohje/lidhje, të cilat mund të japin pista për sjellje të paligjshme, imorale dhe të dyshimta;

• programe (Software):

- ❖ programe për veprime bankare online;
- ❖ programe për llogari/kontabilitet

KONKLUZIONE

Rrezikshmëria që paraqet krimi si një fenomen njerëzor përgjithësisht në botë, kanë bërë të nevojshme për të parë përtej metodave konvecionale ose mjetet tradicionale për parandalimin e kriminalitetit, dhe nga ky punim vihet re dukshëm se përdorimi mjeteve teknologjike janë tashmë një faktor kyq për arritjen e rezultateve efikase dhe të shpejta.

Nga ana tjetër ekspertët ligjorë i kthehen teknologjisë për t'i ndihmuar në çështjet gjyqësore. Në ditët e sotme vihet re dukshëm se, një numër gjithnjë në rritje edhe nga avokatët të cilët kanë përdorur teknologjinë tredimensionale të improvizimit të situatave, apo kriminalistikën mediatike për t'i ndihmuar ekspertët e tyre të paraqesin provat në gjyq.

Ekspertët duke përdorur mjeteve teknologjike bëjnë improvizime grafike dhe hartojnë akte ekspertimi të cilat në bazë të eksperimenteve të ndryshme dhe situatave të ndryshme krijojnë të gjithë dinamikën e ngjarjes dhe mekanizmin se si mund të ketë ndodhur ajo. Shembull tipik i improvizimit me mjete teknike e teknologjike mund të përmendim rastin e një shoferi gjatë një aksidenti me makinë, ku ekspertët me anë të përdorimit të teknologjisë bëjnë të kuptueshme një situatë në të cilën mund të ndihmojnë gjykatën të kuptojnë provat komplekse.

Kuptimi i një situate të veçantë bën të mundur që gjykata të marrë vendimin e duhur rreth asaj që ka ndodhur. Teknologjia është bërë gjithnjë e më e

pranueshme nga drejtësia dhe po lejohet gjithnjë e më shumë në prezantimin e provave, ajo ndikon në përshpejtimin dhe zbulimin e kriminalitetit në vend.

Nga një trajtim i teknologjisë dixhitale vihet re dukshëm se ajo tashmë jo vetëm ndikon në zbulimin dhe parandalimin e kriminalitetit por nga ana tjetër shërben edhe edhe si jë mjet ruajtës i informacioneve duke formuar kështu një arkiv digjital për çdo individ i cili bëhet subjekt i krimit.

Përdorimi i teknologjisë nga organet ligjzbatuese që kanë në funksuion parandalimin dhe zbulimin e krimit është një faktor kyq në ditët e sotme. Midis të tjerave nevojitet një bashkëpunim i ngushtë ndërisnstitucional si në aspektin kombëtar ashtu edhe atë ndërkombëtar për trajtimime të specializuara të subjekteve të cilat kanë detyra të caktuara në parandalimin dhe zbulimin e kriminalitetit.

HUMAN RIGHTS AND TECHNOLOGY

MSC. ENDI KALEMAJ

Student at the Faculty of Law, University of Tirana,
Master of Civil Science
endikalemaj2000@gmail.com

PROF.AC.DR. ERVIS CELA

Professor at the Faculty of Law, University of Tirana,
lawyer in the law firm Çela & Associates Law Firm
erviscela@hotmail.com

Abstract

Human rights are those legal and / or moral rights that all persons have simply as persons. In the current digital age, human rights are increasingly being met or violated in the online environment. a way of conceiving the relationship between human rights and information technology. I propose that we need a Statement of Digital Rights. As a step towards developing such a statement, I suggest a framework for thinking about how to ensure that human rights are met in digital contexts.The rapid evolution of information and communication technology (ICT) and related digital communications over the last two decades has dramatically changed communication practices worldwide. This has had profound implications for human rights on a number of levels. First, communication technologies are presenting new ways to more fully realize our human rights. This is especially true of the right to freedom of expression. Second, ICT has provided human rights activists with

new tools for protecting human rights. Internet access via mobile phones empowers citizens to communicate rights violations in real time with global audiences; social media tools connect human rights defenders around the world to increase collaboration and information sharing; Censorship bypass technologies allow people to bypass attempts to monitor and control the flow of information and communication. However, in addition to unleashing tremendous new opportunities for the protection and advancement of human rights, digital communications also present a number of serious challenges. These include direct threats to human rights, such as the development of increasingly sophisticated censorship and surveillance mechanisms. They also include deeper, structural problems, such as the persistence of digital divisions in access to infrastructure and communication capacities across geographical, gender and social lines[1].The 2017 IEEE report on ethically aligned design for AI lists lists as its first principle that AI design should not violate international human rights. However, some AI systems are already violating rights Like that. For example, in March 2018, human rights investigators from the United Nations (UN) found that Facebook - and the algorithmically driven news source - exacerbated hate speech and instigated violence in Myanmar. During a U.S. Congress hearing in April 2018, Senator Patrick Leahy asked CEO Mark Zuckerberg about Facebook AI's failure to uncover content in the face of possible genocide against Myanmar's ethical Rohingya minority. While Zuckerberg initially told senators that more advanced AI tools would help solve the problem, he later admitted to investors that Facebook's AI systems would not be able to detect "hate" in local contexts accurately. reasonable at any time[2].

Keywords: technology, artificial intelligence, rights, protection, infringement, communication, system.

Entry

The report by the Institute of Electrical and Electronics Engineers, the largest organization of technical professionals, lists as its first principle the non-violation of international human rights by artificial intelligence. However, some systems are already violating such rights. For example, in March 2018, human rights researchers from the United Nations found that

1 https://policycommons.net/artifacts/1340458/information-and-communication-technologies-and-human-rights/1950999/

2 https://datasociety.net/wpcontent/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

Facebook and its algorithmically posted news resulted in the spread of hate speech and incitement to violence in Myanmar. (REUTERS 2018). During a hearing of the US Congress in April 2018, regarding this issue, Zuckenberg initially said that more advanced artificial intelligence is needed to solve the problem[3].

Enforcement of human rights can help identify and anticipate some of the most serious societal violations of artificial intelligence by creating and guiding the creation of technical and political safeguards to promote the most positive use of this intelligence. This can be achieved through the activation of international systems of human rights practices, including EU treaties, United Nations reports and advocacy initiatives to monitor social impacts and establish redress in the event of a violation of these rights.

China is creating systems to categorize people according to their social characteristics. This "Social Credit" system is being created to collect data from Chinese citizens and rate them according to their social credibility, as determined by the government. The system has punitive functions, such as "punishing" debtors, by displaying their faces on large screens in public spaces or by placing these individuals on the "black list" on train or air travel. (The Conversation, 2019¬) A common focus of the country's existing pilot schemes is to establish a standardized system of reward and punishment based on a citizen's credit score. Most pilot cities have used a points system. They all start with a base of 100 points. Citizens can earn bonus points of up to 200 by doing "good deeds", such as getting involved in charity work or sharing and recycling garbage. In the city of Suzhou, for example, you can earn six points for blood donation.

Being a "good citizen" is well rewarded. In some regions, citizens with high social credit scores can enjoy fitness facilities, cheaper public transport, and shorter hospital stays. On the other hand, those with low scores may be restricted from traveling and accessing public services. At this stage, the points are linked to the citizen's identification card number. But the Chinese Internet court has proposed an online identification system linked to social media accounts.

Publishing blacklisted citizens details online is a common practice, but some cities choose to take public shame to another level. Some provinces have used TV and LED screens in public spaces to expose people. In some regions, authorities have remotely personalized blacklisted debtor tones

3 https://www.eurospeak.al/news/fuqia-e-bute/73520-inteligjenca-artificiale-dhe-te-drejtat-e-njeriut/

so that callers hear a message similar to "the person you are calling is a dishonest debtor."[4]

If successful, China's reforms will allow its economy to take the lead in adapting to a dynamic world. But the sheer size of its ambitions (both global and local) also carries the risk that failures, if they occur, could have devastating consequences[5].

Privacy

Privacy has also long been a major concern in areas involving government, business, academia and civil society organizations. The right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), national constitutions and national laws.

If the creators of artificial intelligence were to treat privacy as a fundamental human right, rather than simply an ethical preference, the technical terms and standards of privacy that already exist in the industry would be stronger. The Stanford study gives a brief overview of how artificial intelligence can threaten privacy through rampant data collection and through the ability to publish users anonymously. The protection of the right to privacy is essential for the enjoyment of a number of related rights, such as freedom of expression, of a social life, of participation in political groups, and of the right to information.

Another right that is also violated by artificial intelligence is the right to freedom of expression, which is especially important in an environment where social media platforms, through algorithms, decide "whose voices to listen to." Freedom of expression is part of the fundamental human rights enshrined in Article 19 of the Universal Declaration of Human Rights. Social media platforms have already become the central place where public discussion takes place, but there is a strong debate about the role of platforms in moderating their content. With hate speech, fake news and media manipulation circulating on platforms like Facebook and Twitter, lawmakers and the public are urging companies to address the problem[6].

4 https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963

5 https://theconversation.com/what-we-can-expect-from-chinas-economy-in-2018-89911

6 https://www.eurospeak.al/news/fuqia-e-bute/73520-inteligjenca-artificiale-dhe-te-drejtat-e-njeriut/

It will be inevitable that at some point along the way, humans will interact regularly with robots. Humanoid robots are evolving to do everything from working with astronauts in space to serving as your personal assistant.

Data published by the World Intellectual Property Organization stated that Chinese and American firms hold about 85 percent of the patents belonging to artificial intelligence worldwide. "It's a good thing the EU is looking to legislate on how data can be better used when it comes to personal data, but it should always be up to consumers to decide if their data will be collected and how to distribute them "[7].

Some actors have expressed concern that it will be difficult to define high-risk cases. They are also afraid that the compliance assessment envisaged by the EU will make the process more complex and bureaucratic[8].

The new laws will also have an impact on tech giants like Facebook, Google and Apple. On Monday, Facebook CEO Mark Zuckerberg met with EU officials as the company warned of the potential risks of the innovation regulation.

The Alter 3 robot, which has a human face and hands, which moves its arms very naturally, rotates them during the live performance of Keiichiro Shibuya's opera "Scary Beauty" in the United Arab Emirates, he has replaced the conductor. The role of robots in our daily lives may increase, but it is up to us to decide how artificial intelligence can affect the human experience, where humans and androids create art together.

A survey conducted between four groups of experts in 2012/13 by AI researchers Vincent C Müller and philosopher Nick Bostrom reported a 50% chance that General Artificial Intelligence (AGI) would develop between 2040 and 2050, rising to 90% by 2075. the group went even further, predicting that the so-called 'superintelligence' - which Bostrom defines as "any intellect far exceeding the cognitive performance of humans in almost all areas of interest" - was expected about 30 years later. achieving AGI[9].

However, recent assessments by AI experts are more cautious. Pioneers in the field of modern AI research such as Geoffrey Hinton, Demis Hassabis and Yann LeCun say society is not close to developing AGI. Given the skepticism of the main lights in the field of modern AI and the very different

7 https://www.businessinsider.com/yueh-hsuan-weng-explains-why-robots-need-legal-rights-2015-11

8 https://euronews.al/jetese/2020/02/19/cfare-duhet-te-dini-per-strategjine-e-re-te-be-per-inteligjencen-e-artificiale/

9 https://euronews.al/arte/2020/02/11/roboti-alter-3-qe-drejton-orkestren-njerezore/

nature of modern AI systems close to AGI, there is probably little basis for the fear that a general artificial intelligence will disrupt society in the near future. thus, some AI experts believe that such predictions are extremely optimistic given our limited understanding of the human brain and believe that AGI is still centuries away[10].

Cybercrime

The difficulties of defining cybercrime are also a consequence of the variety of forms through which it is presented and the speed with which it spreads. These commitments have led me to the conclusion that cybercrime does not yet represent a common phenomenological category. Flashing for cybercrime means that the illegal actions were committed using the computer, or these actions could not be committed without the help of the computer. In this category, computer processes are key and they serve to enable, facilitate and expedite the commission of certain criminal acts and yet the computer creates and helps this environment.

During different stages of the development of society, for the causes and character of crime, different and often wrong opinions and findings have been given. Crime as a negative social phenomenon, over different periods of time has been presented in different forms, which have left behind their own special features and characteristics. In this regard, the opinions of the authors in the criminological bridge literature should be supported, in which it is emphasized that: "the volume, forms of crimes and criminal behaviors, have been closely related to the development and transformation of certain societies and systems socio-economic. This process of dependence of forms of crime from specific social transformations is especially observed in contemporary societies, where within short timeframes in different countries, or in the same country, new forms and types of manifestation of crime are observed.

In fact cybercrime should be distanced slightly from a general notion of what is called cybercrime. The latter is related to a criminal activity that has as its object or as a way of committing a crime, the computer. Cybercrime is therefore in this prism a sub-category of cybercrime and is related to criminal activity carried out in the network. The Internet is one of the most global and widely used networks today. After this clarification we can see

10 https://www.zdnet.com/article/what-is-ai-heres-everything-you-need-to-know-about-artificial-intelligence/

that being on the network exposes us to the risk of a possible attack. It would be unprofessional to advise a disconnection from the network, because in today's increasingly global economic structure, disconnection would turn the organism into a non-competitive organism. Another aspect that needs to be addressed to understand the phenomenon of cybercrime is the technology used. An ordinary computer or Internet user, from the moment everything works normally for him, no longer cares what actions, calculations or protocols the computer performs to achieve this result. On the other hand, manufacturers of software, devices, ISPs, etc., do not have a spontaneous will to inform the user about how it works and to be coherent this would be unrealistic. So in conclusion the technology remains more or less non-transparent to the user[11].

Cybercrime is generally understood as a criminal act where computers and networks are the main target, used as tools to commit a crime or are the location of the crime. Although there is no universally accepted definition, a distinction can be made between the two main types of cybercrime: Cybercrime-enabled crime, referring to the 'traditional' forms of crime now transferred to the cyber realm, such as criminal acts focused on finances, acts that impede the safety of children and young people, and even terrorism; Advanced cybercrime (also known as high-tech crime), referring to sophisticated attacks on computer hardware and software. First, it is important not to confuse cybercrime with cyber security[12]. Both cybernetic related threats differ in motive, intent, tools used, targets, scope, consequences, and actors involved in prevention and mitigation. In practice, cybercrime ranges from spam and phishing emails, scams and fraud on the Internet, as well as false representation, to offensive and illegal content, identity theft, and online sexual abuse material. of children. The main motive behind cybercrime, as in the case of 'traditional' crime.

From a legal point of view, the Internet is conceived and functions in such a way that for it the notion of boundaries does not exist. In the legal field a crime is primarily sanctioned by a law. This law belongs to a certain state and is applied by a competent court of a certain state. The notion of state is closely related to the notion of territory, ie state borders. This greatly affects the prosecution phase of the crime. Imagine a computer pirate committing his criminal act from China let's say, attacking a bank in Switzerland and pouring the stolen money electronically into Italy. Which judicial institution and which law is competent in this case? China the country from which the

11 Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime, faqe 21,

12 Përkufizimi i krimit kibernetik sipas Interpolit.

perpetrator committed the crime, Switzerland the country where the victim is located or Italy the country where the result was realized? Will three countries so different in terms of location, legal culture and perception of the notion of crime be able to agree on the prosecution and trial of this act? The answer is not very obvious.

Experience shows that over 50% of attacks target the person. But even if we take into account the organization of the bank separately and the fact of sophisticated software, experience in the field of cybercrime has shown that over 70% of attacks have internal origins. This can come from a dissatisfied subordinate, a subordinate drinking just for profit, and so on. The list of motivations is long[13].

One of the forms of computer misuse is the use of computer for various manipulations. These manipulations consist of entering and recording incorrect data or failing to enter accurate data into the computer, in order to illegally bring material benefits or other benefits to oneself or others. (Vula, 2010) These frauds are numerous in the field of controlling the performance of financial capital and usually appear in the form of fraud related to accounting and banking business, fraud related to investments, insurance, tax liabilities, bankruptcy, money laundering etc. (Vula, 2010) According to the findings of some authors, computer fraud is usually committed through online shopping, ie e-commerce. (Vula, 2010) Computer fraudsters do not choose the means and ways to achieve their goals. Those scams that were previously done in a traditional way, today for such a thing use the computer and the Internet as an efficient and convenient tool, to achieve the goal of gaining material benefit is generally considered to be financial gain. Cybercriminals are, in essence, malicious hackers[14].

"Criminology" was first used by the anthropologist Paul Topinar in the work Anthropology 1879. Rafaello Garafallo first wrote the work criminology 1884 and addressed the phenomenon of crime in society and its causes. Meaning Criminology comes from the Latin word - Greek crime - crime and logos science that d.m.th science on crime in terms of illuminating the forms and causes of its appearance. Criminology - is a science which studies the phenomenon of crime as an individual and social phenomenon by analyzing the forms of its manifestation, illuminating the causes, sources and roots of its economic - social, biopsy nature in order to help prevent and protect of society from this dangerous phenomenon. Crime - the causes

13 https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=1354&context=etd

14 https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=1318&context=etd

of crime have been dependent on the degree of civilization, ideological orientation and professional determination. It is a social phenomenon that since the primitive society the attempts to fight crime are observed, the history of civilization is also related to the history of crime, because the history of crime has for a while aroused fear, insecurity and horror among citizens and at the same time interest . Crime and various criminal behaviors in today's world have become the subject of print and electronic media. Film programs, TVs, video clubs are full of themes and content of crimes, violence, murders and pathological behaviors that bring negative messages by awakening low instincts and the idea of crime, for this reason the question arises from all this interest and preoccupied opinion which we explain by some of the following factors. Subjective and emotional factors - according to the well-known authors Barnes & Beteres, the interest in crime comes from the feeling of fear for life security, moral and sexual integrity, the satisfaction of lusts from the desire to imitate crime.

Computers and networks as the main target When it comes to the most commonly used tools, these include malicious software such as viruses, Trojan horses, adware and spyware to gain access to systems, activity monitoring and data collection; botnets, or hijacked personal computers that perform remote-controlled tasks without the knowledge of their users; and Denial of Service (DoS) attacks, which aim to deplete resources available to a network, application, or service in order to prevent users from accessing them. The effects of such attacks are also manifold. Private individuals may suffer financial losses as well as fall victim to the theft of personal and sensitive information and identity theft. Companies that fall victim to cybercrime face potential financial losses, loss of sensitive operational information, as well as patent data or personal data of their clients and users, all of which can also indirectly result in serious consequences for reputation. Public institutions or non-commercial organizations may become victims of extortion or theft of personal data of users of their services. Computers and networks as tools to commit crime Other criminal acts that are also spreading in the cyber realm include the illicit trafficking of drugs, weapons and sensitive data and information, human trafficking and even murder, beatings and other forms. of contract violence. Generally, such arrangements take place in the so-called 'darknet' where users can operate in complete anonymity. Using the darknet, individuals and criminal organizations use encrypted messaging services to communicate, and cryptocurrencies to conduct financial transactions, making it extremely difficult to track and identify. Hooded hackers (skilled criminals, technicians or technical experts

employed by criminals, see the activation chapter) also exploit the potential of the darknet by exploiting the vulnerabilities of the software they have discovered, selling them anonymously to anyone who seeks them. ways to utilize specific systems[15].

The OSCE, for example, defines cyber terrorism as "Internet-related terrorism and, more specifically, [...], as terrorist attacks on cyber infrastructure, in particular control systems for critical non-nuclear energy infrastructure"[16]. Cyber-terrorism threat scenarios include paralyzing large urban areas, the public health sector, or disrupting the financial sector by "changing some units and some zeros." The rise of the Internet of Things poses another major insecurity that can easily be exploited by terrorist organizations to commit acts of cyber terrorism. Acts of cyber terrorism that would have a physically destructive impact are considered to be unlikely to occur and thus pose less of a challenge to states, due to the enormous amount of resources required to perform such an act. In addition, many terrorist organizations use the Internet to commit traditional crimes, such as fraud, illegal access, and illegal intrusion into computer systems. This results in an overlap between cybercrime (see chapter on cybercrime)[17], cyber attacks (see chapter on cyber warfare) and cyber terrorism; in the end, making it difficult to distinguish between them.

Looking at the extent of cybercrime financial damage, experts rank it in the third place of crime, right after drug trafficking and arms trafficking. The US Department of Justice defines cybercrime as all other criminal activities in which information technology is applied. Just as there are different definitions of cybercrime, there are different divisions of cybercrime[18].

Professor Vodinelic[19] divides cybercrime into 4 major groups:

1. Computer manipulation;

2. Computer espionage (including software theft);

15 https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolALBANIA

16 Udhëzues i praktikave të mira për Mbrojtjen e Infrastrukturës Kritike Energjetike Jo-Bërthamore (NNCEIP) nga sulmet terroriste me fokus te kërcënimet që burojnë nga hapësira kibernetike. 2013. Organizata për Siguri dhe Bashkëpunim në Evropë. Nr.16

17 Cambridge Dictionary e përkufizon "Internet of Things" si objekte që brenda vetes kanë pajisje llogaritëse që mund të lidhen me njëri-tjetrin dhe të shkëmbejnë të dhëna duke përdorur internetin. Interneti i Gjërave po bëhet gjithnjë e më i përfshirë në infrastrukturën kritike kombëtare.

18 Weimann, Gabriel. Mars 2004. https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20 the%20Internet. Raport Special Nr.116. Instituti Amerikan i Paqe

19 Artikull nga Profesori Vodineliq

3. Computer sabotage;

4. Unauthorized use of computer.

Urlich Sieber divides cybercrime into: property offenses, infringement of the right to privacy, and endangering the legally protected interests of others by computer use.

Prof. Asim kovakovi,, starting from the computer system as a central object of cybercrime, divides this type of crime into 3 major groups:

1. Computer misuse (unauthorized access, disclosure of business and other secrets, data corruption, hacking, espionage and computer espionage);

2. Computer-assisted misuse (computer tool for committing computer fraud or computer forgery);

3. Abuses committed by computer (computer piracy - software, computer pornography, provision of goods originating from criminal offenses). Slobodan R. Petrovi bën divides cybercrime based on the basic division of crime into "crime of violence" and "crime of white ties". It could be said that cybercrime belongs to the criminal group of "white ties", although there are forms which belong to the group of violent crime, as well as specific forms of cybercrime. The group of works performed by "white ties" includes:

- Thefts (theft of computers and computer parts, theft of data, theft of passwords, theft of code, etc.);
- Frauds (insurance frauds, taxes and fees, pension funds, social assistance, false presentations, etc.);
- Falsifications (falsification of basic accounting documentation, introduction of fictitious invoices, introduction of fictitious travel accounts, creation of fictitious payment lists, creation of fictitious inventory lists, creation of fictitious buyers, artificial increase of stocks of goods, reflection incorrect loss of goods, falsification of credit reports, creation of false financial data, etc.);
- Forgery (of documents, marks, marks for marking goods, money, signatures, stamps, securities, etc.);
- Violation of privacy (by accessing private computers via the Internet);
- Sabotage (physical and logical);
- Disclosure of secret (state, military, business or official);
- Espionage (disclosure of secret data, rival political activities, plans

and military potential);

- Coercion (through serious threat);
- Blackmail (via email);
- Pornography (photos, animations, files, child pornography, etc.);
- Propaganda (ideological, religious, nationalist, racist, terrorist, spreading false news, etc.)[20]

Conclusions

The number of computer scams is constantly increasing. Cases of computer theft are becoming more and more widespread. According to approximate estimates, during the year the theft of money through the Internet increases many times, both in terms of the extent and in terms of the amount of money stolen. Of particular concern is the fact that, according to incomplete data, about 85% of the perpetrators of computer-assisted fraud have not been detected. According to some authors, a small number of economic crime cases are not detected at all, while an insignificant number of frauds have been reported to the judiciary and prosecuted. There are cases that firms, which have been victims of fraud have not been notified to the competent authorities at all, because their submission would undermine the authority of the firms and would cause even more serious consequences. But there are also more serious cases when criminals blackmail companies that they will destroy computer systems if they do not pay the required amount of money. It happens that a certain firm, through a settlement or directly, pays the amount requested or settled and does not make the case at all. Difficulties in detecting perpetrators of computer fraud also appear because criminals are constantly monitoring the development of information technology and, in parallel, creating and developing new methods of fraud, as well as new ways to protect themselves. Thus, the chances or their detection become even smaller. The very nature of computer-assisted fraud fits. For example, in cases where skilled criminals use the computer to rob banks of money, the offense can only be detected when a business deficit or loss is found, so the perpetrator can be detected late or not detected at all, because is done late.

In the fight against cybercrime, a number of security measures need to be verified, such as:

- Comparison of data of participants in transactions;

20 Artikull nga Prof. Asim Shakoviq

- Verification of data carrier documents;
- Manual and instrumental control of data collection;
- Computer performance verification and computer integrity testing;
- Analysis of expectations, etc.

Computer manufacturers must simultaneously conduct their own investigations and provide answers to how sensitive their production is and what their shortcomings are. At the same time, they need to take protective measures of their systems and adapt the organization to the scale of the technology in the given period, because it develops.

However, there is no absolute security of software, so there is a considerable number of cases of computer manipulation, detected and undetected. What complicates the whole problem even more is the fact that this is a crime whose perpetrators are mainly people with high levels of intelligence and an improvement of the numerous possibilities of information technology. While many forms of classic crime have always been difficult to detect, investigate, prove and convict, information technology today makes this even more difficult. If we add to this the other important fact that most of the operatives, ie investigators, do not have the necessary knowledge, then it is clear how difficult it is to detect cases of cybercrime. For this reason, investigations should be done with a multidisciplinary teamwork. The finding that these acts are difficult to detect should not be discouraged, because the perpetrators of computer fraud can make mistakes through which they can be detected. On the other hand, technology is also sensitive, but it must be well known in order for its shortcomings to be used for good purposes, ie to detect computer fraud.

Bibliography

Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime, faqe 21,

Përkufizimi i krimit kibernetik sipas Interpolit.

Udhëzues i praktikave të mira për Mbrojtjen e Infrastrukturës Kritike Energjetike Jo-Bërthamore (NNCEIP) nga sulmet terroriste me fokus te kërcënimet që burojnë nga hapësira kibernetike. 2013. Organizata për Siguri dhe Bashkëpunim në Evropë. Nr.16

Cambridge Dictionary e përkufizon “Internet of Things” si objekte që

brenda vetes kanë pajisje llogaritëse që mund të lidhen me njëri-tjetrin dhe të shkëmbejnë të dhëna duke përdorur internetin. Interneti i Gjërave po bëhet gjithnjë e më i përfshirë në infrastrukturën kritike kombëtare.

Weimann,Gabriel.Mars2004.https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20 the%20Internet. Raport Special Nr.116. Instituti Amerikan i Paqe

https://policycommons.net/artifacts/1340458/information-and-communication-technologies-and-human-rights/1950999/

https://datasociety.net/ëpcontent/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

https://www.eurospeak.al/news/fuqia-e-bute/73520-inteligjenca-artificiale-dhe-te-drejtat-e-njeriut/

https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963

https://theconversation.com/what-we-can-expect-from-chinas-economy-in-2018-89911

https://www.eurospeak.al/news/fuqia-e-bute/73520-inteligjenca-artificiale-dhe-te-drejtat-e-njeriut/

https://www.businessinsider.com/yueh-hsuan-weng-explains-why-robots-need-legal-rights-2015-11

https://euronews.al/jetese/2020/02/19/cfare-duhet-te-dini-per-strategjine-e-re-te-be-per-inteligjencen-e-artificiale/

https://euronews.al/arte/2020/02/11/roboti-alter-3-qe-drejton-orkestren-njerezore/

https://www.zdnet.com/article/what-is-ai-heres-everything-you-need-to-know-about-artificial-intelligence/

https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=1354&context=etd

https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=1318&context=etd

https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolALBANIA

Artikull nga Prof. Asim Shakoviq

Artikull nga Profesori Vodineliq

EDUKIMI SOCIAL NË KOSOVË PËR ZGJIDHJEN E KONTESTEVE BIZNESORE PËRMES ARBITRAZHIT

PROF.ASOC. ARIF RIZA

Universiteti "Ukshin Hoti"

arif.riza@uni-prizren.com

FATMIR HALILI

Mastër i Shkencave Juridike Ndërkombëtare

fatmir.n.halili@rks-gov.net

fatmir.halili@hotmail.com

Abstract

Nevoja për zgjidhje të shpejta dhe efikase të kontesteve biznesore, ka bërë që të paraqitën edhe procedura alternative, apo jashtëgjyqësore, për zgjidhjen e tyre. Në këtë drejtim, procedurat e arbitrazhit paraqesin një nga format alternative dhe mjaft efikase.

Shoqëria kosovare, duke pasur parasysh proceset e kaluara shtetërore, historinë e okupimit shumëvjeqar dhe moszhvillimin e saj ekonomik, ka bërë që institucionet e saj të jenë të vonshme, e në këtë drejtim edhe të jenë të panjohura deri në vitet e fundit. Në këtë kontekst, procedurat e arbitrazhit kanë filluar të njihen dhe të funksionojnë krejt vonë, dhe në këtë drejtim edhe bizneset janë njohur mjaft vonë me këto procedura.

Në këtë drejtim, punimi trajton nevojën për zgjidhjen alternative të

kontesteve biznesore përmes arbitrazhit në Kosovë, njohjen e bizneseve për rolin e arbitrazhit, besimin e bizneseve në procedurën e arbitrazhit, nevoja për avansimin e legjislacionit për arbitrazh në Kosovë, arbitrazhi si institut i ri për shkollat juridike në Kosovë, etj.

Keywords: Arbitration, Advantages, Disadvantages, Kosovo, Social education, Resolving business disputes, etc.

Introduction

Edukimi shoqëror ka një relevancë të gjerë dhe të shumanshëme. Në veçanti, edukimi shoqëror reflekton drejtpërdrejtë në respektimin e ligjit dhe avancimin e demokracisë. Një shoqëri sa më e shkollar të jetë, është më e avancuar në aspektin e shtetit ligjor dhe demokracisë së atij vendi.

Në këtë kontekst, njohja e legjislacionit dhe respektimi i tij, sjellin edhe efikasitet më të madh në zhvillimin e shoqërisë. Në këtë mënyrë, njohja e bizneseve me procedurat e arbitrazhit paraqet relevanc mjaft të madhe, sepse bizneset nuk do të shkonin në procedura gjyqësore byrokratike ku do të zgjasnin me vite, por do të orientoheshin në procedurat e arbitrazhit, dhe njëkohësisht, kjo do të reflektonte edhe në lehtësimin e gjykatave, sidomos në Kosovë ku gjykatat vazhdojn të kenë mijëra lëndë të grumbulluara që presin zgjidhje.

Në këtë drejtim, shihet qartë edhe nevoja e ekzistencës së arbitrazhit në Kosovë si formë alternative e zgjidhjes së kontesteve biznesore, si edhe avancimi i legjislacionit në këtë fush. Prandaj, trajtimi i kësaj çështje është shumë i nevojshëm nga ekspertët dhe studjuesit për të ofruar njohuri teorike dhe të thelluara për procedurat e arbitrazhit.

1. Themelimi i arbitrazhit në Kosovë

Zhvillimin e arbitrazhit në Republikën e Kosovës mund ta trajtojmë në dy periudha kohore, periudhën para krijimit të shtetit të Kosovës, në veçanti gjatë kohës së ish-Jugosllavisë, dhe periudha e dytë, pas çlirimit të kosovës dhe krijimit të shtetit të pavarur.

Zhvillimi i arbitrazhit në Kosovë gjatë kohës së ish-jugosllavisë

Përderisa Kosova ishte pjesë e ish-Jugosllavisë, deri në përfundimin e këtij shteti flitet posaçërisht në kontekst të federatës, në këtë rast edhe për

arbitrazhin si institucion. Këtu është me rëndësi të përmendet që "edhe pse arbitrazhi mund të duket si një koncept tërësisht i ri për juristët të cilët punojnë në sistemin aktual juridik në Kosovë, aplikimi i arbitazhit daton qysh në fillim të viteve të shtatëdhjeta. Në ish-Jugosllavi, arbitrazhi dhe procedurat e tij ishin një lëndë e rëndësishme që mësohej në fakultetet juridike të të gjitha njësive federative, ndërsa institucionet e arbitrazhit, megjithëse të pakta të numër, merrnin vendime që edhe sot përdoren si precedente nga shumë tribunale të arbitrazhit në mbarë botën[1]. Megjithatë, në Kosovë njohja me procedurat alternative të zgjidhjes së kontesteve biznesore, në këtë rast me procedurat e arbitrazhit, i takon kryesisht periudhës pas përfundimit të luftës më 1999. Arsyet për këtë janë të ndryshme, por nga më të rëndësishmet duhet përmendur, okupimin shumëvjeqar, mungesën e bizneseve të mëdha, shkollimi me përqindje shumë të ulet i shoqërisë, etj.

Zhvillimi i arbitrazhit në Kosovë pas përfundimit të luftës

Që nga përfundimi i luftës dhe vendosja e administratës ndërkombëtare në Kosovë, ishin evidente problemet e shumëta të trashëguara nga ish sistemi, por edhe ato që ishin shkaktuar nga lufta. Kosova nuk kishte vetëm probleme të shkatërrimeve të shkaktuara nga lufta por ekzistoni edhe probleme të shumta pronësore dhe të tjera. Lëndët e shumta të grumbulluara para gjykatave, në një formë ose në një tjetër, e bëjnë të domosdoshme gjetjen e një mënyre për zgjidhjen e këtyre problemeve të grumbulluara. Prandaj, me këtë rast, "me të drejtë është thënë se zgjidhjet alternative të kontesteve kanë lindur në kohë krizash. Zvarritja e zgjidhjes së lëndëve, si dobësi kryesore në sistemet gjyqësore të rajonit, ka bërë që përqindja e rasteve të arbitrazhit dukshëm të rritet"[2].

Në këtë mënyrë, si edhe në të gjitha vendet e tjera, janë paraparë edhe mënyrat alternative për zgjidhjen e kontesteve tregtare, me këtë rast edhe arbitrazhi si një nga këto mënyra.

Megjithkëtë, është e ditur që interesimi për legjislacionin nga fusha ekonomike nuk ishte edhe aq imediat për Kosovën e viteve të pasluftës, andaj edhe ligji për arbitrazhin dhe format e tjera alternative nuk është vënë në rend të parë. Me mbështetje nga USAID në Kosovë Sistemi për Përmbarimin e Marrëveshjeve dhe Vendimeve (SEAD), dy institucione në Kosovë, Oda Ekonomike e Kosovës (OEK) dhe Oda Ekonomike Amerikane Programi i USAID-it në Kosovë për përmbarim dhe legjislacion komercial

1 Programi i USAID-it në Kosovë për përmbarim dhe legjislacion komercial, nëntor 2014, fq. 16

2 http://www.kosovo-arbitration.com/sq_AL/blog/lajme-1/post/pse-duhet-ti-themi-po-arbitrazhit-ne-kosove-9 - 08.02.2022

në Kosovë (American Chamber), themeluan programet e ZAK-ut, Tribunali i Përhershëm i Arbitrazhit (TPA) pranë OEK-së dhe Qendra pë Zgjidhjen Alternative të Kontesteve (ZAK) pranë Odës Ekonomike Amerikane ne Kosovë"[3].

2. Nevoja për arbitrazh në Kosovë

Natyrisht që gjykatat mbetën ndër mekanizmat më të popullarizuar për zgjidhjen e problemeve të ndryshme shoqërore, me këtë rast edhe të kontesteve me karakter ekonomik. Mirëpo, ekzistojnë arsye të mjaftueshëme që krahas gjykatave disa çështje të gjejnë zgjidhje edhe përmes formave të tjera alternative, siç është edhe arbitrazhi. Posaçërisht, është evidente pas luftës në Kosovë, që ekzistojnë konteste të shumëta të akumuluara në gjykata, si dhe zvarritja e tyre nga neglizhenca e gjyqëtarëve, kanë bërë edhe më të nevojshëm zhvillimin e formave alternative për zgjidhjen e kontesteve. Por, shkuarja në arbtrazh, ende nuk shihet serioze dhe zgjidhje adekuate nga bizneset në Kosovë, kjo për faktin, që palët nuk janë të njoftuara siç duhet me institucionin e arbitrazhit. Me këtë rast, vlen të përmendet që institucioni i arbitrazhit krejt vonë ka filluar të trajtohet në teori dhe të bëhet i njohur tek bizneset, siç edhe ka filluar të bëhet pjesë e studimit në universitetet e vendit.

Gjithashtu, është me rëndësi të përmendet se, në dekadën e fundit, ndër sfidat e raportuara nga bizneset në vazhdimësi dhe në veçanti lidhur me zbatimin e kontratave, paraqitet funksionimi jo i kënaqshëm i gjykatave. Bazuar në rezultatet një hulumtimi mbi gjendjen e bizneseve në Kosovë, të realizuar në vitin 2014, vetëm 5% të respondentëve janë deklaruar se sistemi gjyqësor është efikas, përderisa 38% e shohin si joefikas, në krahasim me 57% që e shohin si mesatarisht efikas[4]. Në këtë drejtim, ky është një tregues mjaft i mirë se sa ka nevoj për orientim të zgjidhjes së kontesteve biznesore përmes procedurave të arbitrazhit.

Prandaj, me të drejtë potencohet se përdorimi i arbitrazhit ende është i pakët në Republikën e Kosovës, sepse bizneset dhe shoqëria kosovare nuk është e njoftuar mirë me atë se çfarë është arbitrazhi dhe çfarë ofron arbitrazhi. Megjithatë, avansimi i arbitrazhit dhe fillimi i zgjidhjes së kontesteve përmes kësaj mënyre alternative veç më ka filluar.

---

3 Programi i USAID-it në Kosovë për përmbarim dhe legjislacion komercial, nëntor 2014, fq. 16-17

4 Studim Vjetor i Qendrës së Arbitrazhit, Qendra e Arbitrazhit në Odën Ekonomike Amerikane në Kosovë, Shtator 2016, fq. 4

3. Njohja e bizneseve për rolin e arbitrazhit

Roli i arbitrazhit në zgjidhje të kontesteve mbetet i padiskutueshëm. Që nga paraqitja e arbitrazhit e deri në ditët e sotme, procedurat e arbitrazhit janë perfeksionuar vazhdimisht, dhe roli i tij sot është i ngjashëm me procedurat gjyqësore, për më tepër, ka arsye të konsiderohet edhe më i mirë se procedurat gjyqësore.

Kosova pas përfundimit të luftës më 1999, ka filluar zhvillimin e saj në aspektin e ekonomisë së tregut nga ekonomia centraliste dhe mjaft e cunguar nga okupimi shumëvjeqar. Në këtë drejtim, edhe funksionimi i bizneseve dhe tregtis si brenda ashtu edhe me vendet tjera, ka qenë mjaft primitiv dhe i pa organizuar si duhet.

Fillimi i organizimit ligjor të mirëfillt ka filluar me prezencën ndërkombëtare. Nënshtrimi i bizneseve rregullave të ekonomis së tregut ka filluar me nxjerrjen e rregulloreve të UNMIK-ut, të cilat deri në shpalljen a pavarësisë së Kosovës më 17 Shkurt 2008, kanë pasur fuqi legjislative, dhe me miratimin e ligjeve të reja nga Kuvendi i Kosovës kanë pushuar të vlejnë si të tilla.

Duke pasur parasysh këtë, bizneset në Kosovë kanë qenë shumë pak të informuara për funksionimin ligjor të ekonomis së tregut, e në këtë drejtim, fare pak me procedurat e arbitrazhit, dhe mundësitë që ofrohen përmes këtyre procedurave për zgjidhje të kontesteve biznesore. Kjo mosnjohje e bizneseve me procedurat e arbitrazhit në Kosovë, është pa dyshim rrjedhoj edhe e funksionimit të bizneseve të vogla dhe individuale, dhe mugesës së kompanive të mëdha.

4. Pse arbitrazhi dhe jo gjykata?

Dallimet midis Arbitrazhit dhe Gjykatave është mjaft i qartë. Para së gjithash është e rëndësishme të theksohet që gjykatat janë organe shtetërore, ndërsa, arbitrazhi paraqet një organ i cili është i themeluar me marrëveshjen e palëve, gjë që nënkupton, se nëse nuk ekziston marrëveshja midis palëve për arbitrazh, në fakt nuk ekziston as arbitrazhi.

Sa herë që flitet për arbitrazh, është gati e pamundur të mos bëhet krahasimi me gjykatat. Kjo për faktin se, arbitrazhi shihet si një procedurë 'rivale' ndaj procedurave gjyqësore. Por, që të dyja procedurat kryejn të njëjtin funksion. Në këtë drejtim, me të drejtë shkruan edhe autori shqiptar Mejdi Hetemi se, "për nga vështrimi, si gjykata po ashtu edhe arbitrazhi kryejnë funksion të

njëjtë juridiko-gjykimore dhe se vendimet e tyre përfundimtare gëzojnë fuqi të njëjtë juridike"[5]. Në këtë drejtim, kur theksohet se, si procedurat gjyqësore, po ashtu edhe arbitrazhi kryejn funksione të njëjta, atëherë shtrohet me të drejtë pyetja: pse arbitrazhi dhe jo gjykatat? ose dhe e kundërta. Në këtë rast, vlen të përmendet se, gati të gjithë autorët që trajtojnë procedurat e arbitrazhit, këto procedura i shohin me përparësi më të madhe krahasuar me procedurat gjyqësore. Në këtë kontekst vlen të përmendet edhe konstatimi i autorit Kalia i cili thekson se "arbitrazhi paraqitet gjithnjë e më shumë si mjet i shpejtë më pak i kushtueshëm për gjykimin e një çështjeje sesa gjykatat e zakonshme, si dhe njëkohësisht si mjet për arritjen e një drejtësie të vërtet, duke eliminuar ndërkohë, papërshtatshmëritë apo anomalitë e ndodhura gjatë gjykimit nga një gjyqtar i zakonshëm"[6]. Po ashtu, vlen të përmendet edhe konstatimi i autorit tjetër Mauro Rubino-Sammartano, i cili thekson se arbitrazhi është një mekanizëm që ndryshon nga procedurat gjyqësore, meqë ndër avantazhet e tjera arbitri zgjidhet nga palët dhe procedurat pritet të jenë me kohëzgjatje më të shkurtër dhe se qëllimi i procedurave të arbitrazhit është të arrihet: saktësi, drejtësi, efikasiteti dhe një vendim i zbatueshëm[7].

Po ashtu, nuk do të thotë se arbitrazhi është perfekt kundrejtë procedurave gjyqësore, tek të gjithë autorët që trajtojnë këtë temë, përmenden edhe mugesat apo disavantazhet që kanë procedurat e arbitrazhit kundrejt atyre gjyqësore. Në këtë drejtim, përmenden si mungesa apo disavanazhe të procedurave të arbitrazhit si: arbitër të pakualifikuar, mungesa e besueshmërisë nuk ka shkallë të dytë në arbitrazh, arbitrazhi është punë dytësore, korrupsioni i mundshëm i arbitrit ose trupit të arbitrave[8]. Mirëpo, ajo që vlen të përmendet është se, shumica e autorëve parashohin më shumë përparësi dhe zgjidhje më të mirë të kontesteve biznesore përmes procedurave të arbitrazhit, krahasuar me procedurat gjyqësore.

Ajo që del nga trajtimet e autorëve të ndryshëm për procedurat e arbitrazhit, dhe përparësitë e këtyre procedurave, që autorët përmendin, kundrejtë procedurave gjyqësore janë: mundësia e zgjedhjes së arbitrave (gjyqtarëve) nga palët sipas dëshirës së tyre; profesionalizmi (ekspertiza) e lartë e arbitrave; kredibiliteti dhe autoriteti i tyre i pakontestueshëm; neutraliteti

5 Mehdi J. Hetemi, ARBITRAZHI, Kolegji AAB, Prishtinë, 2015, fq. 24

6 Ardian Kalia, E Drejta ndërkombëtare private, Tiranë, 2010, fq.336

7 Mauro Rubino-Sammartano, International Arbitration Law and Practice, Third Edition, Juris Publishing, Inc, 2014, fq. 52

8 Valbon Mulaj, The Advantages and Disadvantages of Arbitration in Relation to the Regular Courts in Kosovo, Hungarian Journal of Legal Studies 59, No 1, pp. 118–133, Akadémiai Kiadó, Budapest, 2018, fq. 129

i arbitrave; efikasiteti (shpejtësia e procedimit) dhe efektiviteti i gjykimit (procedurës së arbitrazhit); fleksibiliteti i arbitrazheve, kushtueshmeria (kostoja) e gjykimit; procedurat dhe vendimet e arbitrazhit janë kryesisht jo publike (konfidenciale) që është relevante për bizneset; etj. Në këtë rast, është e udhës të përmendet se, "argument mjaft prezent në disfavor të përzgjedhjes së arbitrazhit mbetet mungesa e procedurës së ankesës, dhe përceptimi se vendimi gjyqësor është më fuqiplotë në raport me vendimin e arbitrazhit. Edhe pse mekanizmi i apelit nëpër institucionet e arbitrazhit nuk është pothuajse fare prezent, me përjashtim të ICSID dhe ICC, dhe Qendra e Arbitrazhit nuk synon të themeloj një procedurë të tillë, rezulton se shumica e bizneseve do të donin që një shkallë e apelit të ishte në dispizicion për ta"[9].

5. Besimi i bizneseve në procedurën e arbitrazhit

Kur kemi parasysh mungesën e njohurive për procedurat e arbitrazhit, pa dyshim, edhe besimi në zgjidhjen e mosmarrveshjeve biznesore përmes kësaj procedure është shumë i zbehtë. Gjithashtu, duke pasur parasysh se procedura e arbitrazhit është private, dilemat për ekzekutimin e vendimit të arbitrazhit kanë ekzistuar çdo herë tek bizneset.

Natyrisht, prirja për tu besuar organeve shtetërore ka luajtur rol mjaft të madh në këtë drejtim. Duke konsideruar që pas vendimit të organit shtetëror ekziston edhe manifestimi i forcës, gjë që nuk e kanë strukturat joshtetërore.

Sidoçoftë, kjo është në tërësi nga mosnjohja e procedurave të arbitrazhit dhe legjislacionit pozitiv. Pra, rol të posaçëm në këtë drejtim ka luajtur edukimi shoqërorë – juridik, dhe mos informimi i duhur me legjislacionin e shtetit. Në këtë kontekst, "megjithë kritikat e vazhdueshme ndaj gjyqësorit, arbitrazhi mbetet pak i përdorur nga bizneset. Në mes tjerash, barriera në përdorimin e arbitrazhit janë raportuar të jenë mungesa e informatave lidhur me këtë mekanizëm; shqetësimi lidhur me mungesën e një shkalle të ankimimit; si dhe hezitimi i bizneseve që të jenë nismëtar të përdorimit të këtij mekanizmi, ende duke e konsideruar si periudhë testuese"[10]. Pa dyshim, kjo është edhe rrjedhoj e tranzicionit shoqërorë nëpër të cilin po kalon edhe sot e kësaj dite Kosova.

9 Studim Vjetor i Qendrës së Arbitrazhit, Qendra e Arbitrazhit në Odën Ekonomike Amerikane në Kosovë, Shtator 2016, fq. 15

10 Studim Vjetor i Qendrës së Arbitrazhit, Qendra e Arbitrazhit në Odën Ekonomike Amerikane në Kosovë, Shtator 2016, fq. 4

6. Arbitrazhi – institut i ri për shkollat juridike në Kosovë

Përveç paraqitjes së vonshme të procedurave të arbitrazhit në Kosovë, edhe interesimi për këto procedura nga shkollat juridike është i vonshëm. Në faqet e internetit të universiteteve dhe kolegjeve, shohim lëndën e procedurave të arbitrazhit, si lëndë opcinale, ose trajtohet brenda lëndëve të tjera, si për shembull, në kuadër të së drejtës tregtare, apo të drejtës ekonomike.

Veq tjerash, edhe autorët e shkencave juridike shumë pak, për të mos thënë fare, janë marr me studimin dhe hulumtimin e procedurave të arbitrazhit. Në këtë drejtim, Mehdi Hetemi ka shkruar për procedurat e arbitrazhit dhe format tjera alternative në kuadër të librit "E Drejta Ndërkombëtare Tregtare-afariste"[11] të botuar më 2007, ndërsa Asllan Bilalli ka publikuar një punim në revistën e botuar nga Fakulteti Juridik i Universitetit të Prishtinës në vitin 2011[12], më vonë në vinin 2015, autori tjetër Iset Morina ka botuar librin me titull "Arbitrazhi Dhe Procedura e Arbitrazhit"[13], të gjithë këta autor janë profesor të rregullt në Fakultetin Juridik të Universitetit të Prishtinës. Nga kjo, rrjedh se shkollat juridike në Kosovë dhe autorët kosovarë, mjaft vonë kanë filluar të trajtojnë procedurat e arbitrazhit, gjë që, tregon se edhe edukimi shoqëror dhe bizneset vonë kanë filluar të njohin procedurat e arbitrazhit.

7. Nevoja për avansimin e legjislacionit për arbitrazh në Kosovë

Kosova është nënshkruese e disa marrëveshjeve bilaterale dhe multilaterale në fushën e arbitrazhit. Me këtë rast vlen të theksohet që Kosova si një nga shtetet pasuese të Republikës Socialiste Federative të Jugosllavisë i ka njohur në mënyrë të njëanshme konventat ndërkombëtare të ratifikuara nga Republika Socialiste Federative e Jugosllavisë. Në këtë formë, për shembull, sa i përket çështjes së vendimeve të arbitrazheve të huaja, ligji për ndryshimin dhe plotësimin e ligjit për Procedurën Kontestimore, me të cilin shtohet neni 511, ka përcaktuar se: Njohja dhe ekzekutimi i vendimeve të huaja të arbitrazhit do të zbatohet në përputhje me Konventën New York për njohjen dhe ekzekutimin e vendimeve të huaja të Arbitrazhit[14]. Po ashtu,

11 Mehdi Hetemi, E Drejta Ndërkombëtare Tregtare-afariste, Prishtinë, 2007

12 Asllan BILALLI, E Drejta, Revistë për Çështje Juridike dhe Shoqërore, Viti XXXV - nr.3-4 – 2011

13 Iset Morina, Arbitrazhi dhe Procedura e Arbitrazhit, Prishtinë, 2015

14 LIGJI NR. 04/L-118 PËR NDRYSHIMIN DHE PLOTËSIMIN E LIGJIT NR. 03/L-006 PËR

Konventa për Zgjidhjen e Mosmarrëveshjeve të Investimeve midis Shteteve dhe Shtetasve të Shteteve të tjera e vitit 1965, Konventa e ICSID, e hyrë në fuqi për Republikën e Kosovës më 29 korrik 2009.

Është e rëndësishëme të theksohet që Kosova tashmë ka edhe ligjin e miratuar nga Kuvendi i Kosovës për arbitrazhin. Ky ligj është miratuar në Kuvend më 26. 01. 2007, dhe është shpallur me Rregulloren e UNMIK-ut nr. 2008/30, datë 05.06.2008. Gjithashtu, Kuvendi i Odës Ekonomike të Kosovës, duke u bazuar në nenet 8(k), 17(g) dhe (h), 24, 26 dhe 27 të Ligjit Nr. 2004/7 për Odën Ekonomike të Kosovës; me qëllim të organizimit të një arbitrazhi të përhershëm kompetent për zgjidhjen e kontesteve të biznesit në mes të anëtarëve të Odes Ekonomike të Kosovës dhe në mes të anëtarëve dhe personave të tjerë juridik ose fizikë, më 24 qershor 2011, miraton rregullat e arbitrazhit të Kosovës.

Gjithashtu, vlen të përmendet se, në shtator 2008, hyri në fuqi Ligji për Arbitrazhin e Kosovës (Ligji Nr. 02/L-75) (Ligji për Arbitrazhin), i cili bazohet në Ligjin Model të UNCITRAL-it. Ky ligj konsiderohet se i plotëson kërkesat formale dhe përmbajtësore të ligjit modern të arbitrazhit, dispozitat e tij kanë karakter lex specialis në lidhje me Ligjin për Procedurën Kontestimore në lidhje me procedurën e arbitrazhit. Ligji për Arbitrazhin rregullon arbitrazhin vendor dhe ndërkombëtar dhe përcakton procedurat për zbatimin e vendimeve të arbitrazhit vendor (neni 38) dhe të huaj (neni 39). Ligji për Investimet e Huaja (Ligji Nr. 04/L220), i miratuar në vitin 2014, favorizon edhe më tej përdorimin e arbitrazhit në marrëdhëniet ndërkombëtare[15]. Në këtë drejtim, në aspektin përmbajtësor, ligji ka ende nevoj për tu plotësuar dhe ndryshuar, për të ofruar më shumë efikasitet. Duhet pasur parasysh se shumë ligje në Kosovë janë bërë shpejtë dhe pa ndonjë ekspertizë të gjerë, po ashtu, shumica e ligjeve janë përkthim bukfal i ligjeve të shteteve të ndryshme, gjë që nuk i përgjigjen gjendjes reale socio-ekonomike të Kosovës. Prandaj, edhe rishikimi dhe plotësimi i legjislacionit është i domosdoshëm. Veq tjerash, vlen të theksohet se, ende ka nevoj për trajnimin e arbitrave të rinjë dhe specializimin e tyre për zgjidhjen e çështjeve biznesore.

PROCEDURËN KONTESTIMORE, GAZETA ZYRTARE E REPUBLIKËS SË KOSOVËS / Nr. 28 16 TETOR 2012, PRISHTINË

15 Christian W. Konrad, Konrad & Partners & Virtyt Ibrahimaga, International Arbitration, fourth edition, Published by Global Legal Group Ltd. 59 Tanner Street, London SE1 3PL, United Kingdo, 2018, fq. 228

Conclusions

Nga trajtimi i tematikës për edukimin shoqëror në drejtim të zgjidhjes së kontesteve biznesore përmes procedurave të arbitrazhit, mund të nxjerrim disa konkluza.

- Kosova është shtet i ri, ende ndodhet në ndërtim të institucioneve të saja, si dhe në drejtim të avancimit të tyre. Në këtë drejtim, okupimi shumëvjeqar dhe tranzicioni shoqëror ka bërë që shumë çështje të jentë të panjohura për shoqërinë. Andaj, edhe procedurat e arbitrazhit si metod alternative e zgjidhjes së kontesteve biznesore, ka filluar të përdoret mjaft vonë.
- Edukimi dhe ngritja e nivelit të vetëdijes shoqërore, shkollimi i mirëfilltë, janë gjithashtu faktor shumë i rëndësishëm në respektimin e ligjit, dhe funksionimin e institucioneve, në këtë drejtim, edhe reflektimi dhe njohja me procedurat alternative të zgjidhjes së kontesteve biznesore, në këtë rast procedurat e arbitrazhit.
- Njohja e bizneseve më procedurat e arbitrazhit si metod mjaft efikase në zgjidhjen e kontesteve biznesore, gjithashtu është e vonshme, e që ka ardhur si rrjedhoj e ekzistimit të bizneseve të vogla dhe individuale, tek të cilat kontestet biznesore kanë ekzistuar shumë pak, dhe gjithashtu, edhe nga mos interesimi i studjuesve dhe shkollave juridike për format alternative të zgjidhjes së kontesteve biznesore.
- Krahasimi i legjislacionit kosovar për procedurat e arbitrazhit me legjislacionet e vendeve të zhvillluara, na jep pasqyrë të qartë se, legjislacioni i Kosovës ka nevoj për plotësim, ndryshim dhe avansim të mëtejshëm, bazuar edhe në atë se ligji për arbitrazhin i Kosovës është përshtatur tërësisht me ligjin Model të UNCITRAL-it i cili është reviduar, ndërsa ligji i Kosovës është bazuar në versionin e parë të tij.
- Si përfundim, synimi i këtij punimi është të elaboroj mungesën e shkollimit të mirëfillt shoqërorë dhe impaktet që ka shkollimi i shoqërisë, konkretisht shoqërisë kosovare, në zhvillimin e procedurave të arbitrazhit si një nga procedurat alternative të zgjidhjes së kontesteve biznesore.

Reference:

Mehdi J. Hetemi, ARBITRAZHI, Kolegji AAB, Prishtinë, 2015,

Ardian Kalia, E Drejta ndërkombëtare private, Tiranë, 2010,

Mauro Rubino-Sammartano, International Arbitration Law and Practice, Third Edition, Juris Publishing, Inc, 2014,

Arif Riza, E Drejta e Organizatave Ndërkombëtare dhe Organizatat Ndërkombëtare, Prishtinë 2011

Valbon Mulaj, The Advantages and Disadvantages of Arbitration in Relation to the Regular Courts in Kosovo, Hungarian Journal of Legal Studies 59, No 1, pp. 118–133, Akadémiai Kiadó, Budapest, 2018,

Christian W. Konrad, Konrad & Partners & Virtyt Ibrahimaga, International Arbitration, fourth edition, Published by Global Legal Group Ltd. 59 Tanner Street, London SE1 3PL, United Kingdo, 2018,

Ligji nr. 04/l-118 për ndryshimin dhe plotësimin e ligjit nr. 03/l-006 për procedurën kontestimore, gazeta zyrtare e republikës së kosovës / nr. 28 16 tetor 2012, prishtinë

Programi i USAID-it në Kosovë për përmbarim dhe legjislacion komercial, nëntor 2014,

Studim Vjetor i Qendrës së Arbitrazhit, Qendra e Arbitrazhit në Odën Ekonomike Amerikane në Kosovë, Shtator 2016,

http://www.kosovo-arbitration.com/sq_AL/blog/lajme-1/post/pse-duhet-ti-themi-po-arbitrazhit-ne-kosove-9 - 08.02.2022

POLITIKAT E NEVOJSHME TATIMORE DHE FINANCIARE NE KOHË KRIZASH

DR. EJONA BARDHI
Pedagoge, Fakulteti i Drejtësisë, Universiteti i Tiranës
Departamenti i së Drejtës Publike
ejona.bardhi@fdut.edu.al

Abstrakt

Një krizë është një dukuri komplekse natyrore dhe shoqërore dhe për shkak të këtij fakti jepen përkufizime dhe interpretime të ndryshme në shkrimet për këtë temë. Brenda menaxhimit të krizave, kriza shikohet si një ndryshim dramatik dhe negativ i rutinës, që e bën atë sfidën tjetër me të cilën përballen njerëzit, shoqëria dhe shkenca. Pra kriza është një luhatje e kohës, një gjendje e gjërave kur një ndryshim thelbësor është i pashmangshëm dhe përmban dy mundësi: njëra është e lidhur me një rezultat të padëshiruar, negativ dhe tjetri me një rezultat të duhur ekstrem pozitiv. Shanset janë zakonisht të barabarta, por ne mund t'i ndryshojmë ato. Pavarësisht nga burimi i krizës, nëse është një fenomen natyror, aktiviteti njerëzor ose pasiviteti dhe pa marrë parasysh se çfarë lloji është shkatërrues ose jo, i papritur, në zhvillim ose i qëndrueshëm ai kalon nëpër disa faza. Në menaxhimin e krizave pika kyçe është "parandalimi" dhe përqendrimi i përpjekjeve kryesore intelektuale, morale, sociale dhe teknologjike gjatë periudhës para krizës. Qëllimi kryesor është parandalimi i efekteve që janë negative për njerëzit. Në fakt, ky parandalim në mënyrë figurative mund të quhet meditim mbi të paparashikueshmen, njohjen e së panjohurës, planifikimin e së papriturës. Është mirë të dihet se në këtë mënyrë e ardhmja dhe, përkatësisht, ngjarjet e ardhshme bëhen më pak të papritura, të panjohura dhe të paparashikueshme. Kjo, nga ana e saj, na jep një shans për të sfiduar

realitetin në mënyrë më efektive. Pikërisht punimi do të orientohet në sfidat dhe tejkalimin e menaxhimit në kohë krize, duke u njohur me këto sfida, mënyrën si menaxhohen ato dhe si tajkalohet ky menaxhim.

Fjalë Kyçe: krizë, dukuri, menaxhim, masa, tejkalim, parandalim.

NECESSARY TAX AND FINANCIAL POLICIES IN TIMES OF CRISIS

DR. EJONA BARDHI

Lecturer, Faculty of Law, University of Tirana

Department of Public Law

ejona.bardhi@fdut.edu.al

Abstract

A crisis is a complex natural and social phenomenon and due to this fact different definitions and interpretations are given in the writings on this topic. Within crisis management, crisis is seen as a dramatic and negative change of routine, which makes it the next challenge faced by people, society and science. So crisis is a fluctuation of time, a state of affairs when a fundamental change is inevitable and contains two possibilities: one is associated with an unwanted, negative outcome and the other ëith a proper extreme positive outcome. The odds are usually equal, but we can change them. Regardless of the source of the crisis, whether it is a natural phenomenon, human activity or passivity and no matter ëhat type it is destructive or not, sudden, evolving or sustainable it goes through several stages. In crisis management the key point is the "prevention" and concentration of key intellectual, moral, social and technological efforts during the pre-crisis period. The main goal is to prevent effects that are negative for humans. In fact, this prevention figuratively can be called meditation on the unpredictable, recognizing the unknown, planning the unexpected. It is good to know that in this way the future and, respectively, future events become less unexpected, unknoën

and unpredictable. This, in turn, gives us a chance to challenge reality more effectively. Exactly the work will be oriented to the challenges and overcoming the management in times of crisis, getting acquainted with these challenges, the way they are managed and how this management is overcome.

Keywords: crisis, occurrence, management, measures, overcoming, prevention.

1.Politika monetare në kohë krize

Efektet e politikës monetare gjatë krizave financiare ndryshojnë thelbësisht nga ato në kohë normale. Politika monetare ka efekte më të mëdha dhe më të shpejta gjatë krizave financiare mbi prodhimin dhe inflacionin, dhe gjithashtu në variabla të tjerë të ndryshëm makroekonomikë si kredia, çmimet e aktiveve, pasiguria dhe besimi i konsumatorit. Efektet në prodhim dhe inflacion janë veçanërisht të forta gjatë fazës akute të krizave financiare kur ekonomia është gjithashtu në recesion, ndërsa ato janë më të dobëta gjatë fazës së rimëkëmbjes pasuese. Gjithashtu ka ndryshime në madhësinë dhe kohën e veprimeve të politikës monetare gjatë krizës financiare globale të 2008/09 midis vendeve që mund të kenë kontribuar në performancën e ndryshme makroekonomike në të gjithë vendet.[1] Gjatë krizës financiare globale që filloi në 2007, shumë banka qendrore lehtësuan politikën monetare në mënyrë agresive në mënyrë që të lehtësonin shqetësimin e tregut financiar, të rritnin prodhimin dhe të stabilizonin inflacionin. Politika monetare ishte kryesisht e suksesshme në zbutjen e shqetësimit të tregut financiar, por rritja e prodhimit dhe inflacioni mbetën më të ulëta se sa pritej në shumë ekonomi të përparuara dhe rikuperimet u perceptuan gjerësisht si të ngadalta dhe zhgënjyese[2]. Këto vëzhgime çuan në një debat me bazë të gjerë nëse kanalet e transmetimit të politikës monetare ishin dëmtuar për shkak të krizës financiare globale dhe nëse politika monetare në përgjithësi është më pak efektive gjatë krizave financiare dhe pasojave të tyre[3]. Rëndësia e këtij debati tejkalon nevojën e përgjithshme të bankave qendrore për vlerësimin e efektivitetit të politikave të tyre. Crucshtë thelbësore për

1 Monetary Policy during Financial Crises: Is the Transmission Mechanism Impaired? Nils Jannsen,a Galina Potjagailo, and Maik H. Woltersa, Kiel Institute for the World Economy. University of Kiel, University of Jena, MFS at Goethe-University Frankfurt. Aksesuar https://www.ijcb.org/journal/ijcb19q4a3.pdf

2 Shih, për shembull, Pain et al. 2014.

3 Shih, për shembull, Bouis et al. 2013.

përcaktimin e një përzierjeje politike që mund të stabilizojë ekonominë gjatë krizave financiare. Nëse politika monetare është më pak efektive në kriza të tilla, lindin pyetjet nëse duhet të sigurohen stimuj më të mëdhenj monetarë për të arritur efektet e dëshiruara; nëse politikat e tjera, siç është politika fiskale, duhet të përdoren më gjerësisht; ose nëse rimëkëmbjet e ngadalta pas krizave financiare duhet të tolerohen duke pasur parasysh se ka pak hapësirë për politikën monetare. Në këtë drejtim, çështja e efektivitetit të politikës monetare gjatë krizave financiare është gjithashtu e rëndësishme për vlerësimin e efekteve anësore të padëshirueshme, të tilla si marrja e tepërt e rrezikut dhe flluskat e çmimit të aseteve, që mund të ndodhin nëse politika monetare mbetet shumë e zgjerur për një periudhë të zgjatur kohe[4]. Krizat financiare shfaqin disa karakteristika që mund të ndikojnë në transmetimin e politikës monetare: shqetësimi i lartë i tregut financiar, paqëndrueshmëria dhe pasiguria makroekonomike, besimi i ulët i pjesëmarrësve të tregut dhe rregullimet thelbësore të bilancit të firmave dhe familjeve. Të gjitha këto karakteristika të pafavorshme mund të dëmtojnë transmetimin e politikës monetare. Në veçanti, bankat mund të mos jenë të gatshme të zgjasin furnizimin e tyre të kreditit, sepse ato përballen me rrezik më të lartë të mospërmbushjes së kredisë dhe sepse u duhet të rregullojnë bilancet e tyre pas humbjeve të mëparshme[5]. Gjithashtu, krizat financiare paraprihen në mënyrë tipike nga flluska të çmimeve të aktiveve dhe bumeve të kreditit dhe konsumit dhe, si pasojë, zakonisht ndiqen nga heqja e borxheve të ekonomive familjare dhe firmave dhe rritja e neveritjes ndaj rrezikut[6]. Prandaj, në periudha të tilla, oferta dhe kërkesa për kredi mund të mbetet e dobët, pavarësisht nga norma e interesit e vendosur nga autoriteti monetar, duke penguar kështu kanalin e kredisë të politikës monetare. Kanali i normës së interesit të politikës monetare mund të dëmtohet, sepse në kohë pasigurie të lartë investitorët mund të shtyjnë vendimet e pakthyeshme të investimeve derisa të vijnë më shumë informacione[7]. Pasiguria pastaj bëhet përcaktuese kryesore e vendimeve për investime, ndërsa politika monetare humbet ndikimin e saj[8]. Në mënyrë të ngjashme, reagimi i normës së interesit të investimeve mund të bjerë kur firmat dhe konsumatorët kanë besim të ulët në biznesin e tyre ose perspektivat e punësimit (Morgan 1993). Së fundmi, mund të bëhet më e vështirë për bankat qendrore të stabilizojnë

4 Shih, p.sh., Rajan 2005; Altunbasa, Gambacorta dhe Marques-Ibanez 2014; Jim´enez et al. 2014.

5 Bouis et al. 2013; Buch, Buchholz dhe Tonzer 2014; Valencia 2017.

6 Reinhart dhe Rogoff 2008.

7 Shih, p.sh., Bernanke 1983; Dixit dhe Pindyck 1994

8 Bloom, Bond dhe Reenen 2007.

prodhimin sepse në kohë të paqëndrueshmërisë së lartë makroekonomike firmat priren të rregullojnë çmimet e tyre më shpesh (Vavra 2014). Nga ana tjetër, një ndërhyrje e politikës monetare mund të jetë gjithashtu veçanërisht efektive, nëse mund të zbusë disa nga karakteristikat e krizës financiare të pafavorshme dhe në këtë mënyrë të parandalojë reagimet e kundërta midis sektorit financiar dhe ekonomisë reale, duke rivendosur kështu funksionimin e kredisë dhe interesit kanali i normës[9]. Në veçanti, kufizimet e kredisë kanë më shumë gjasa të lidhen gjatë krizave financiare, duke çuar në një rritje të primit të jashtëm të financave. Politika monetare në këtë situatë mund të jetë në gjendje të ulë primin e financave të jashtme duke lehtësuar kufizimet e kredisë, në mënyrë që përshpejtuesi financiar i Bernanke, Gertler dhe Gilchrist (1999) të bënte politikën monetare veçanërisht efektive. Për më tepër, ndërsa është më pak efektive në prani të shqetësimit dhe pasigurisë së lartë të tregut financiar, politika monetare mund të jetë gjithnjë e më e fuqishme nëse është në gjendje të lehtësojë ndjeshëm shqetësimin e tregut financiar dhe të zvogëlojë pasigurinë[10]. Në mënyrë të ngjashme, politika monetare mund të jetë më efektive nëse është në gjendje të rrisë besimin nga nivele shumë të ulëta, duke siguruar sinjale për perspektivat e ardhshme ekonomike[11], duke ulur probabilitetin e rezultateve në rastin më të keq dhe duke përmirësuar aftësinë e agjentët për të bërë vlerësime të probabilitetit në lidhje me ngjarjet në të ardhmen (Ilut dhe Schneider 2014) .[12] Katastrofa natyroret janë shpesh ato që sjellin krizat më të mëdha ekonomike dhe që mund të shkaktojë një konflikt midis dy objektivave që janë objekt monitorimi dhe rregullimi midis qeverisë dhe Bankës së Shqipërisë. Nga njëra anë, rritja e njëkohshme të çmimeve, pra inflacionit dhe nga ana tjetër tendencat afatshkurtra për ulje të tendencës rritëse të ekonomisë. U takon Bankës së Shqipërisë dhe Ministrisë së Financave, që të dyja të harmonizuara në politikat dhe objektivat të rivlerësojnë objektivat dhe të ndjekin rrjedhën më të mirë të veprimit. Për shkak se fluksi fillestar i inflacionit pas një katastrofe është i përkohshëm, i lokalizuar dhe i përqendruar në sektorë të veçantë, politika monetare duhet të ndikojë në mbajtjen e inflacionit të ulët. Edhe nëse Banka e Shqipërisë do të donte të kontrollonte inflacionin, nuk mund ta bëjë këtë pa rritur ndjeshëm normat e interesit pasi politika monetare synon të gjithë ekonominë, e cila do të ushtronte presion të mëtejshëm në një

9 Shih, p.sh., Mishkin 2009.

10 Bekaert, Hoerova dhe Lo Duca 2013; Basu dhe Bundick 2017.

11 Barsky dhe Sims 2012.

12 Bachmann and Sims (2012) provide evidence that the confidence channel is important for the effectiveness of fiscal policy in stimulating economic activity. Similar effects are conceivable in the context of monetary policy.

ekonomi tashmë të ngadalësuar. Mbajtja e politikës monetare ekspansioniste do të siguronte në këtë kontekst likuiditet shtesë për sistemin financiar dhe do të mbante besimin e lartë pas pasigurisë që sjell katastrofa.

Sidoqoftë, si niveli i interesit para katastrofës ashtu edhe niveli i inflacionit mund të kufizojnë përdorimin e politikës monetare. Por, ndërkohë Banka e Shqipërisë edhe mund të ulë normat e interesit për të stimuluar shpenzimet që ndikohen prej interesit, siç janë investimet kapitale dhe konsumi i mallrave dhe shërbimeve të përditshme dhe bazë.

2. Masat e politikës fiskale dhe ekonomike në kohë krizash

Në kohën e çrregullimeve të ekuilibrit në mes të ofertës dhe kërkesës së gjthmbarshme në kohë krize, shteti duhet ta zvogëlojë patjetër kërkesën e vet, kurse në kohën e zvogëlimit të kërkesës, shteti duhet të rrisë patjetër shpenzimet e veta në mënyrë që të ndikojë në rritjen e kërkesës së gjithanshme. Me një fjalë shteti duhet ta percjellë me kujdes ofertën dhe kërkesën në mënyrë që ta ruajë ekuilibrin, andaj kjo quhet politikë fiskale anticiklike. Ndryshimet në llojin dhe në lartësinë e të hyrave dhe të shpenzimeve publike zakonisht bëhen me aplikimin e:

(1) stabilizatorit automatik (të inkorporuar),

(2) formulës së elasticitetit dhe

(3) masave diskrete.

Me nocionin stabilizator automatik (i inkorporuar), nënkuptohen ato të hyra publike dhe shpenzime publike të cilat reagojnë automatikisht, pa ndikimin e drejtpërdrejtë të shtetit, në ndryshimet në sferën private dhe në këtë mënyrë i zbusin efektet e ndryshimeve të ofertës dhe të kërkesës së gjithmbarshme. Vendi më i rëndësishëm në mesin e stabilizatorëve automatik i takon tatimit në të ardhura, me rastin e aplikimit të të cilit përdoren përqindjet progresive. Në të vërtetë, gjatë hovit ekonomik bëhet rritja e të ardhurave të subjekteve ekonomike dhe rritja e kërkesës. Për shkak të përqindjeve progresive të aplikuara me rastin e tatimit të të hyrave rritet ngarkimi tatimor i obliguesve tatimorë më shpejt sesa është rritja e të ardhurave në dispozicion, e kjo ndikon pozitivisht në stabilizimin në ekonomi. Në kohën e depresionit në ekonomi aplikimi i tatimit progresiv në të ardhurat ndikon në rritjen më të shpejtë të përqindjes së shpenzimeve publike dhe të të hyrave publike.[13]

13 Prof.Dr.Bozhidar Jelçiq ,Fakulteti Juridik-Universiteti i Kosovës në Prishtinë Shkenca mbi financat

Këtu është e nevojshme të theksohet në menyrë të veçantë se për efektet stabilizuese të stabilizatorëve automatikë (të inkorporuar) mund të flitet vetëm atëherë kur teprica e të hyrave publike, që është bërë në kohën e hovit ekonomik, përjashtohet nga qarkullimi, përkatesisht në qoftë se mungesa e të hyrave që ndodh në kohën e depresionit në ekonomi plotësohet me mjetet e huas, financimi deficitar. Në shpenzimet publike rolin e stabilizatorit automatik e kanë dhëniet e ndryshme sociale në radhë të parë kompensimet në të holla për të papunët në kohën e recesionit, shteti paguan nga buxheti nga fondet e ndryshme etj. Shuma më të mëdha në emër të ndihmës sociale, e kjo ndikon pozitivisht në rritjen e kërkesës private (e me këtë edhe në rritjen e prodhimit), kurse në kohën e prosperitetit ekonomik bëhet zvogëlimi i dhënieve sociale, përkatesisht paraqiten tepricat në këtë sektor të shpenzimeve publike, e kjo do të ndikojë në kufizimin e kërkesës, e me këtë do të ndikojë në drejtim të stabilizimit në ekonomi. Që të sigurohet mundësia më e madhe e shfrytëzimit të stabilizatorit automatik, në buxhet duhet t'u sigurohet një vend më i dukshëm atyre të hyrave dhe shpenzimeve që do të kenë efekt automatik stabilizues. Mirëpo, duhet të vërejmë se shfrytëzimi i stabilizatorit automatik nuk mund zëvendësojë (plotësisht) masat e tjera të politikës aktive konjukturore anticiklike të shtetit. Në kushtet bashkëkohëse krahas stabilizatorëve automatikë aplikohen edhe masat e tjera të politikës fiskale që të pengohen, përkatësisht të kufizohen çrregullimet në ekonomi.

Me nocionin e formulës së elasticitetit nënkuptohen masat që janë të orientuara kah pengimi, përkatësisht kah eliminimi i pasojave të çrregullimeve në ekonomi. Sipas konceptit të aplikimit të formulës së elasticitetit duhet të sigurohet automatizmi i caktuar në eliminimin e pasojave të ecurive të papërshtatshme në ekonomi. Në të vërtetë, me dispozita përcaktohen masa të caktuara të cilat duhet të ndërmerren në domenin e politikës tatimore dhe të politikës së të hyrave publike në përgjithësi në përqindjen e punësisë, në nivelin e çmimeve, në rritjen e të ardhurave kombëtare, ose në disa madhësi të tjera agregate të caktuara më parë. Kështu p.sh, në rast të rritjes së nivelit të çmimeve për 10% automatikisht do të rritet ngarkimi tatimor për përqindje të caktuar, përkatësisht do të zvogëlohen shpenzimet publike. Masat diskrete të politikës fiskale kanë vendin më të rëndësishëm ndër masat e politikës fiskale, ndër masat bashkëkohëse të politikës së stabilizimit. Ky emërtim përdoret për ato masa që organet kompetente shtetërore, sipas vlerësimit të vet, i ndërmarrin për realizimin e stabilizimt ekonomik ad hoc, do të thotë, me ndërmarrjen e masave të caktuara që nuk janë të përcaktuara

dhe e drejta financiare-botues enti i teksteve dhe mjeteve Prishtinë 1985.përkthyes –Mr.Sabri Kadriu. faqe- 661 - 662.

që më parë. Rëndom, për ndërmarrjen e masave diskrete të politikës fiskale janë të autorizuara organet ekzekutive, qeveria ose ministritë (ministrat) kompetentë. Në qoftë se këto masa janë në kompetencën e parlamentit (kuvendit), nevojitet një kohë më e gjatë (që të reagohet ndaj dukurive të caktuara për shkak të procedurës relativisht komplekse, të gjatë, të punës së forumit përfaqësues dhe të organeve të tij.[14]

3. Politika monetare në kohë krize

Efektet e politikës monetare gjatë krizave financiare ndryshojnë thelbësisht nga ato në kohë normale. Politika monetare ka efekte më të mëdha dhe më të shpejta gjatë krizave financiare mbi prodhimin dhe inflacionin, dhe gjithashtu në variabla të tjerë të ndryshëm makroekonomikë si kredia, çmimet e aktiveve, pasiguria dhe besimi i konsumatorit. Efektet në prodhim dhe inflacion janë veçanërisht të forta gjatë fazës akute të krizave financiare kur ekonomia është gjithashtu në recesion, ndërsa ato janë më të dobëta gjatë fazës së rimëkëmbjes pasuese. Gjithashtu ka ndryshime në madhësinë dhe kohën e veprimeve të politikës monetare gjatë krizës financiare globale të 2008/09 midis vendeve që mund të kenë kontribuar në performancën e ndryshme makroekonomike në të gjithë vendet.[15]

Gjatë krizës financiare globale që filloi në 2007, shumë banka qendrore lehtësuan politikën monetare në mënyrë agresive në mënyrë që të lehtësonin shqetësimin e tregut financiar, të rritnin prodhimin dhe të stabilizonin inflacionin. Politika monetare ishte kryesisht e suksesshme në zbutjen e shqetësimit të tregut financiar, por rritja e prodhimit dhe inflacioni mbetën më të ulëta se sa pritej në shumë ekonomi të përparuara dhe rikuperimet u perceptuan gjerësisht si të ngadalta dhe zhgënjyese[16]. Këto vëzhgime çuan në një debat me bazë të gjerë nëse kanalet e transmetimit të politikës monetare ishin dëmtuar për shkak të krizës financiare globale dhe nëse politika monetare në përgjithësi është më pak efektive gjatë krizave financiare dhe pasojave të tyre[17]. Rëndësia e këtij debati tejkalon nevojën e përgjithshme

14 Prof.Dr.Bozhidar Jelçiq ,Fakulteti Juridik-Universiteti i Kosovës në Prishtinë Shkenca mbi financat dhe e drejta financiare-botues enti i teksteve dhe mjeteve Prishtinë 1985.përkthyes –Mr.Sabri Kadriu.faqe 653-656.

15 Monetary Policy during Financial Crises: Is the Transmission Mechanism Impaired? Nils Jannsen,a Galina Potjagailo, and Maik H. Woltersa, Kiel Institute for the World Economy. University of Kiel, University of Jena, MFS at Goethe-University Frankfurt. Aksesuar https://www.ijcb.org/journal/ijcb19q4a3.pdf

16 Shih, për shembull, Pain et al. 2014.

17 Shih, për shembull, Bouis et al. 2013.

të bankave qendrore për vlerësimin e efektivitetit të politikave të tyre. Crucshtë thelbësore për përcaktimin e një përzierjeje politike që mund të stabilizojë ekonominë gjatë krizave financiare. Nëse politika monetare është më pak efektive në kriza të tilla, lindin pyetjet nëse duhet të sigurohen stimuj më të mëdhenj monetarë për të arritur efektet e dëshiruara; nëse politikat e tjera, siç është politika fiskale, duhet të përdoren më gjerësisht; ose nëse rimëkëmbjet e ngadalta pas krizave financiare duhet të tolerohen duke pasur parasysh se ka pak hapësirë për politikën monetare. Në këtë drejtim, çështja e efektivitetit të politikës monetare gjatë krizave financiare është gjithashtu e rëndësishme për vlerësimin e efekteve anësore të padëshirueshme, të tilla si marrja e tepërt e rrezikut dhe flluskat e çmimit të aseteve, që mund të ndodhin nëse politika monetare mbetet shumë e zgjerur për një periudhë të zgjatur kohe[18]. Krizat financiare shfaqin disa karakteristika që mund të ndikojnë në transmetimin e politikës monetare: shqetësimi i lartë i tregut financiar, paqëndrueshmëria dhe pasiguria makroekonomike, besimi i ulët i pjesëmarrësve të tregut dhe rregullimet thelbësore të bilancit të firmave dhe familjeve. Të gjitha këto karakteristika të pafavorshme mund të dëmtojnë transmetimin e politikës monetare. Në veçanti, bankat mund të mos jenë të gatshme të zgjasin furnizimin e tyre të kreditit, sepse ato përballen me rrezik më të lartë të mospërmbushjes së kredisë dhe sepse u duhet të rregullojnë bilancet e tyre pas humbjeve të mëparshme[19]. Gjithashtu, krizat financiare paraprihen në mënyrë tipike nga flluska të çmimeve të aktiveve dhe bumeve të kreditit dhe konsumit dhe, si pasojë, zakonisht ndiqen nga heqja e borxheve të ekonomive familjare dhe firmave dhe rritja e neveritjes ndaj rrezikut[20].

Prandaj, në periudha të tilla, oferta dhe kërkesa për kredi mund të mbetet e dobët, pavarësisht nga norma e interesit e vendosur nga autoriteti monetar, duke penguar kështu kanalin e kredisë të politikës monetare. Kanali i normës së interesit të politikës monetare mund të dëmtohet, sepse në kohë pasigurie të lartë investitorët mund të shtyjnë vendimet e pakthyeshme të investimeve derisa të vijnë më shumë informacione[21]. Pasiguria pastaj bëhet përcaktuese kryesore e vendimeve për investime, ndërsa politika monetare humbet ndikimin e saj[22]. Në mënyrë të ngjashme, reagimi i normës së interesit të investimeve mund të bjerë kur firmat dhe konsumatorët kanë

18 Shih, p.sh., Rajan 2005; Altunbasa, Gambacorta dhe Marques-Ibanez 2014; Jim´enez et al. 2014.

19 Bouis et al. 2013; Buch, Buchholz dhe Tonzer 2014; Valencia 2017.

20 Reinhart dhe Rogoff 2008.

21 Shih, p.sh., Bernanke 1983; Dixit dhe Pindyck 1994

22 Bloom, Bond dhe Reenen 2007.

besim të ulët në biznesin e tyre ose perspektivat e punësimit (Morgan 1993). Së fundmi, mund të bëhet më e vështirë për bankat qendrore të stabilizojnë prodhimin sepse në kohë të paqëndrueshmërisë së lartë makroekonomike firmat priren të rregullojnë çmimet e tyre më shpesh (Vavra 2014). Nga ana tjetër, një ndërhyrje e politikës monetare mund të jetë gjithashtu veçanërisht efektive, nëse mund të zbusë disa nga karakteristikat e krizës financiare të pafavorshme dhe në këtë mënyrë të parandalojë reagimet e kundërta midis sektorit financiar dhe ekonomisë reale, duke rivendosur kështu funksionimin e kredisë dhe interesit kanali i normës[23]. Në veçanti, kufizimet e kredisë kanë më shumë gjasa të lidhen gjatë krizave financiare, duke çuar në një rritje të primit të jashtëm të financave. Politika monetare në këtë situatë mund të jetë në gjendje të ulë primin e financave të jashtme duke lehtësuar kufizimet e kredisë, në mënyrë që përshpejtuesi financiar i Bernanke, Gertler dhe Gilchrist (1999) të bënte politikën monetare veçanërisht efektive. Për më tepër, ndërsa është më pak efektive në prani të shqetësimit dhe pasigurisë së lartë të tregut financiar, politika monetare mund të jetë gjithnjë e më e fuqishme nëse është në gjendje të lehtësojë ndjeshëm shqetësimin e tregut financiar dhe të zvogëlojë pasigurinë[24]. Në mënyrë të ngjashme, politika monetare mund të jetë më efektive nëse është në gjendje të rrisë besimin nga nivele shumë të ulëta, duke siguruar sinjale për perspektivat e ardhshme ekonomike[25], duke ulur probabilitetin e rezultateve në rastin më të keq dhe duke përmirësuar aftësinë e agjentët për të bërë vlerësime të probabilitetit në lidhje me ngjarjet në të ardhmen (Ilut dhe Schneider 2014) .[26]

Katastrofa natyroret janë shpesh ato që sjellin krizat më të mëdha ekonomike dhe që mund të shkaktojë një konflikt midis dy objektivave që janë objekt monitorimi dhe rregullimi midis qeverisë dhe Bankës së Shqipërisë. Nga njëra anë, rritja e njëkohshme të çmimeve, pra inflacionit dhe nga ana tjetër tendencat afatshkurtra për ulje të tendencës rritëse të ekonomisë. U takon Bankës së Shqipërisë dhe Ministrisë së Financave, që të dyja të harmonizuara në politikat dhe objektivat të rivlerësojnë objektivat dhe të ndjekin rrjedhën më të mirë të veprimit.

Për shkak se fluksi fillestar i inflacionit pas një katastrofe është i përkohshëm, i lokalizuar dhe i përqendruar në sektorë të veçantë, politika

23 Shih, p.sh., Mishkin 2009.

24 Bekaert, Hoerova dhe Lo Duca 2013; Basu dhe Bundick 2017.

25 Barsky dhe Sims 2012.

26 Bachmann and Sims (2012) provide evidence that the confidence channel is important for the effectiveness of fiscal policy in stimulating economic activity. Similar effects are conceivable in the context of monetary policy.

monetare duhet të ndikojë në mbajtjen e inflacionit të ulët. Edhe nëse Banka e Shqipërisë do të donte të kontrollonte inflacionin, nuk mund ta bëjë këtë pa rritur ndjeshëm normat e interesit pasi politika monetare synon të gjithë ekonominë, e cila do të ushtronte presion të mëtejshëm në një ekonomi tashmë të ngadalësuar. Mbajtja e politikës monetare ekspansioniste do të siguronte në këtë kontekst likuiditet shtesë për sistemin financiar dhe do të mbante besimin e lartë pas pasigurisë që sjell katastrofa.

Sidoqoftë, si niveli i interesit para katastrofës ashtu edhe niveli i inflacionit mund të kufizojnë përdorimin e politikës monetare. Por, ndërkohë Banka e Shqipërisë edhe mund të ulë normat e interesit për të stimuluar shpenzimet që ndikohen prej interesit, siç janë investimet kapitale dhe konsumi i mallrave dhe shërbimeve të përditshme dhe bazë.

KONKLUZIONE DHE REKOMANDIME

1.Krijoni një plan të menaxhimit të krizave.

Kjo duhet të përfshijë formimin e një ekipi të përkushtuar ndër-funksional. Një grup i rëndësishëm, i udhëhequr zakonisht nga Eprori më I lartë në nivel hierarkik, i cili duhet të udhëheqë, të japë përparësi dhe të koordinojë përpjekjet për të vlerësuar situatën dhe për të zhvilluar një plan të menaxhimit të krizave. Plani i menaxhimit të krizave duhet të përfshijë veprimet që organizata duhet të bëjë për të vazhduar funksionimin, për të arritur misionin e saj të interesit publik dhe për të lehtësuar ndikimin e krizës. Në zhvillimin e planit, siguria e individëve duhet të jetë përparësia kryesore dhe duhet të jetë lenta/llupa me të cilën është hartuar plani i menaxhimit të krizave.

Megjithëse shumë organizata/biznese/institucione nuk kanë një plan zyrtar, ose kanë plane që nuk janë azhurnuar kohët e fundit, nuk është kurrë vonë për të organizuar një plan të tillë dhe për të vepruar.

2. Ekzekutoni planet për të punuar në mënyrë virtuale.

Nëse organizata/biznesi/institucioni nuk është duke punuar tashmë në mënyrë virtuale, duhet që kjo kohë të përdoret për të planifikuar. Edhe pse shumica e organizatave kanë qenë të njohura me takimet virtuale, është krejt ndryshe të jesh në një mjedis plotësisht virtual. Ka shumë aspekte që duhet të merren parasysh, duke filluar nga mënyra se si të bëhen lidhjet virtuale sa më efektive dhe efikase, deri te sfidat praktike dhe çështjet e shëndetit

mendor të cilat vijnë si pasojë e punës nga shtëpia[27].

3. Krijoni një strategji komunikimi.

Në një krizë, ekziston pashmangshmërisht frika dhe pasiguria. Komunikimi i shpeshtë i informacionit të rëndësishëm mund ta lehtësojë këtë, si dhe të sigurojë një ndjenjë lidhjeje dhe rehatie në këto kohë shumë të vështira. Çdo organizatë/biznes/institucion duhet të planifikojë të komunikojë me stafin, anëtarët, vullnetarët, dhe aktorët e tjerë relevant. Komunikimet për stafin duhet të pranojnë që frika gjatë kësaj kohe është normale, ndërsa ndihmojnë gjithashtu që të gjithë të kenë një kuptim të qartë të qëllimeve dhe përparësive. Komunikimet me anëtarët prsh tek bzinesi duhet t'i ndihmojnë ata të vazhdojnë aktivitetet e tyre profesionale. Për shembull, komunikimet me firmat mund të përqendrohen në shtyerjen e afatave për deklarimin e tatimeve ose ndonjë ndryshim tjetër legjislativ dhe rregullativ që mund të ndikojnë në to. Komunikimet gjithashtu mund t'i inkurajojnë ata të marrin parasysh shërbimin që mund t'i ofrojnë publikut gjatë krizës.

4. Pajisni anëtarët tuaj me burime.

Bota jonë virtuale ofron një mori burimesh që mund të jenë shumë të dobishme për të ndihmuar anëtarët përmes çdo krize. Ato duhet të synojnë nevojat e sektorëve të ndryshëm të anëtarësisë së tyre: firma të mëdha dhe të vogla, kontabilistë në biznes, edukator, studentë, kontabilistë të sektorit publik, etj. Vendimarrësit duhet të jenë të pajisur për të mbështetur klientët e tyre/ komunitetin e tyre të cilët gjithashtu mund të preken nga kriza. Në biznes shumë firma më të mëdha kanë prodhuar tashmë materiale të mira që mund të shpërndahen. Gjithashtu, mjete të ndryshme të mësimit në mënyrë virtuale janë në dispozicion që mund të ndihmojnë. Sektorët e tjerë mund të kenë nevoja të ndryshme që duhet të synohen në përputhje me rrethanat.[28]

5. Planifikimi i planit emergjent për skenarë të ndryshëm,

Veçanërisht ato të përqendruara rreth vazhdimësisë së biznesit. Është e

27 The Harvard Business Review "Një udhëzues për menaxhimin e punëtorëve tuaj nga distanca".

28 IFAC ka lansuar një faqe në internet për të shpërndarë burime rreth COVID-19 i cili përmbanë informacione nga organizata, Forumi i Firmave dhe aketrët e tjerë relevant, si dhe informacione nga vetë IFAC, për të na ndihmuar të gjithë ne të ndajmë përvojat dhe njohuritë në kohë krize.

rëndëishme të shikoni përpara dhe të merrni parasysh "çfarë nëse". Prsh edhe pse koronavirusi është më i frikshëm për kërcënimin ndaj shëndetit dhe sigurisë, ai gjithashtu ka një ndikim serioz, potencialisht shkatërrues, ekonomik. Çdokush në kohë krize duhet të marrë parasysh prioritetet e saj strategjike në mjedisin e ri, në çfarë duhet të përqendrohet dhe se çfarë mund të shtyhet për më vonë. Pastaj duhet të marrë në konsideratë, bazuar në krizën dhe prioritetet e biznesit, cilat janë ndikimet afatshkurtra dhe afatgjata në të ardhurat, shpenzimet dhe rrjedhën e parave. Përderisa disa shpenzime mund të reduktohen, një subjekt mund të marrë në konsideratë të investojë në mënyra të reja për të mbështetur anëtarët, siç është zhvillimi i programeve online. Gjithashtu duhet të azhurnohen planet e menaxhimit të rrezikut.

6. Bashkëpunimi.

Profesioni global i kontabilitetit dhe auditimit është një rrjet i mahnitshëm që mund të bashkohet në çdo krizë. Duhet të merret në konsideratë bashkëpunimi me aktorët relevant, të cilët mund të përfshijnë agjencitë qeveritare dhe të donatorëve, organizatat ndërkombëtare dhe kombëtare, rregullatorët, institucionet financiare, etj. Kontaktimi i aktorëve relevant paraqet një mundësi për të shkëmbyer informacione dhe i hap rrugën konsiderimit të mundësive për të bashkëpunuar për iniciativa. Në disa vende, qeveritë janë duke formuar grupe të aktorëve relevant për administrimin e krizave kombëtare. Kur është e mundur, duhet të konsiderojnë anëtarësimin në grupe të tilla për të ofruar perspektivat dhe mbështetjen nga profesioni i kontabilitetit dhe auditimit. Ato të cilat kanë hasur vështirësi në kalimin nga ofrimi i shërbimeve në person në ofrimin e shërbimeve në mënyrë virtuale brenda një periudhe të shkurtër kohore duhet t'iu drejtohen organizatave të tyre rajonale si dhe kontakteve për marrëdhëniet me publikun për të kërkuar asistencë.[29]

29 Linda Lach, Darlene Nzorubara, (Prill, 2020), "*SHTATË HAPA TË RËNDËSISHËM PËR PLANIFIKIMIN E MENAXHIMIT TË KRIZËS PËR OPK-TË*". Aksesuar online https://www.ifac.org/knowledge-gateway/developing-accountancy-profession/discussion/shtat-hapa-t-r-nd-sish-m-p-r-planifikimin-e-menaxhimit-t-kriz-s-p-r-opk-t

PEGASUS – THE GOOD, THE BAD, THE EVIL

DR. IVAS KONINI[1]

DR. GENADA TAHO[2]

Abstract

Pegasus is commonly known as the world's most powerful cyber-weapon. Developed by three Israeli friends, the NSO Group, the Trojan horse promise that it could do what no one else could do: consistently and reliably crack the encrypted communications of any iPhone or Android smartphone. For more than a decade, it had helped Mexican authorities capture the drug lord known as El Chapo and more than 40 countries have quietly used Pegasus to thwart terrorist plots, fight organized crime and identifying hundreds of several crime suspects. In a sense, NSO's products seemed to solve one of the biggest problems facing law-enforcement and intelligence agencies in the 21st century: that criminals and terrorists had better technology for encrypting their communications than investigators had to decrypt them.

Unfortunately, since 2019, the many abuses of Pegasus had also been well documented: Mexico deployed the software not just against gangsters but also against journalists and political dissidents. The United Arab Emirates used the software to hack the phone of a civil rights activist whom the government threw in jail. Saudi Arabia used it against women's rights activists and, to spy on communications with Jamal Khashoggi, a journalist for The Washington Post, whom Saudi operatives killed in 2018.

Cyber-weapons have changed international relations more profoundly than any advance since the advent of the atomic bomb. In some ways, they are even more profoundly destabilizing — they are comparatively cheap, easily distributed and can be deployed without consequences to the attacker. Nowadays more than 45 countries of the world (as far as public information)

1 email : ivas.konini@fdut.edu.al

2 email : genada.taho@fdut.edu.al

use Pegasus to turn the nation's smartphones into an "intelligence gold mine."

Key words: Pegasus, NSO Group, human rights, zero click attack, cybersecurity.

Hyrje

Në ditët e sotme njerëzimi është i varur në mënyrë të paprecendentë nga interneti, si për të zgjeruar një biznes, për të zhvilluar veprime të ndryshme financiare, madje edhe për të kryer detyra që mbajnë të dhëna sensitive.Ky lum informacionesh është vazhdimisht i disponueshëm për t'u aksesuar nga hakerat nëpërmjet programeve të ndryshme.

Shumë prej nesh janë të vetëdijshëm se sulmet kibernetike janë rritur në mënyrë eksponenciale gjatë dy viteve të fundit. Si individët, ashtu dhe bizneset kanë vënë re informacione dhe të dhëna kritike të kompromet uara për shkak të hakerëve që infektojnë pa mëshire pajisjet e tyre.

Aktualisht, në rrjetin ndërkombëtar që është përfshirë në fushatën e zbulimit të hakerimeve, po bën bujë hetimi i programit zbulues "Pegasus".Ai është quajtur si sulmi "më i sofistikuar ndonjeherë" ndaj një smartphone-i. Disa madje i kanë vënë pseudonimin "Pegasus - përgjimi perfekt", duke u kthyer kështu në një çështje tepër shqetësuese për Shtetet e Bashkuara të Amerikës, Mbretërinë e Bashkuar, Francën, Gjermaninë e shumë shtete të tjera të fuqishme.

Kreu I

1.1 Origjina e programit "Pegasus"

"Pegasus" është projektuar dhe zhvilluar nga NSO Group[3], një kompani izraelite që shet pajisje survejuese shtetërore të nivelit të parë ushtarak.NSO e merr emrin nga Niv, Shalev dhe Omri, tre themeluesit e saj.Nga këta, Shalev, i cili është edhe Drejtori Ekzekutiv, ka shërbyer si Major në Forcat e Mbrotjes Izraelite (në Njësinë e Kërkimit dhe Shpëtimit).Madje, kompania pretendon që stafi i saj përbëhet nga veteranë dhe elitarë të ndryshëm të agjensive të inteligjencës[4].

3 https://www.nsogroup.com/

4 https://www.vice.com/en/article/wnxpjm/nso-group-new-big-player-in-government-spyware

"Pegasus" është teknologjia përgjuese më e avancuar në botë pasi përdor tenikën me zero klikim për infektim. Pra, jo vetëm që nuk kërkohet që përdoruesi i smartphone-it (viktima) të klikojë diçka, por virusi mund të shkarkohet automatikisht përmes një mesazhi (nuk ka rendësi nëse ai/ajo e lexon ose jo atë), ose një telefonate anonime (nuk ka rendësi nëse ai/ajo i përgjigjet asaj), të cilat vetëshkatërrohen, duke e bërë të pamundur që viktima ta kuptojë që tashmë po përgjohet dhe mbikëqyret. Gjithashtu, vështirësia për ta zbuluar qëndron edhe në faktin se "Pegasus" nuk mund të gjendet në asnjë folder në telefon, nuk mund të kapet përmes programeve anti-virus, si edhe nuk shkakton as ngadalësim dhe as mbinxehje të pajisjes ku shkarkohet.Emërtimi "Pegasus" vjen nga figura mitologjike greke e kalit të pavdekshëm me krahë, sepse ai është një virus kompjuterik që mund të dërgohet "duke fluturuar nëpër ajër" për të infektuar telefonat celularë[5].

1.2 A është "Pegasus" një risi "e mirë" apo "e keqe" në fushën e përgjimit dhe mbikëqyrjes?

Në faqen e saj zyrtare, Kompania NSO tregon që misioni i saj është të shpëtojë jetë dhe të krijojë një botë më të mirë dhe më të sigurt.Ajo premton që teknologjitë e saj përdoren vetëm ligjërisht, nga qeveri të huaja, për të hetuar dhe parandaluar terrorizmin dhe krimin. Kjo kompani qartësisht thekson se produktet e saj përdoren eskluzivisht nga agjensitë shtetërore të inteligjencës së huaj dhe agjensitë e zbatimit të ligjeve, nëpërmjet blerjes së licensës, me qëllim për të luftuar krimin dhe terrorizmin. Aktualisht Kompania NSO ka rreth 60 përdorues në 40 shtete, nga të cilët 38% janë njësi të zbatimit të ligjit, 51% janë agjensi të inteligjencës dhe 11% janë ushtarakë[6].

Vetë kompania deklaron[7] që përpara se ta shesë licensën për "Pegasus", kërkuesi kalon në një "Vetting" gjithëpërfshirës për të vërtetuar nëse ky i fundit shkel ose jo, abuzon ose jo me të drejtat dhe liritë themelore të njeriut. Nëse pas këtij kontrolli dhe verifikimi del se kërkuesi as nuk i shkel dhe as nuk abuzon me të drejtat dhe liritë themelore të njeriut, shitja e licensës duhet të kalojë edhe një fazë tjetër, ajo duhet të miratohet paraprakisht nga Ministria Izraelite e Mbrojtjes[8], nëpërmjet një kontrate me agjensitë qeveritare të huaja "për përdorim eskluzivisht ligjor dhe vetëm për qëllim të

5 https://en.wikipedia.org/wiki/"Pegasus"_(spyware)

6 https://www.businesstoday.in/technology/news/story/"Pegasus"-spyware-is-the-nso-groups-technology-good-or-evil-301878-2021-07-20

7 https://www.nsogroup.com/about-us/

8 https://www.vice.com/en/article/wnxpjm/nso-group-new-big-player-in-government-spyware

parandalimit dhe hetimit të krimeve madhore dhe akteve terroriste".

"Pegasus" nuk mund të përdoret për përgjimin e numrave amerikanë.Për këtë, kohët e fundit është zhilluar "Phantom", simotra e "Pegasus".Në fokus të saj është vetëm përgjimi i numrave telefonikë amerikanë.

Modeli i kontratës që firmoset ndërmjet Kompanisë NSO dhe shtetit kërkues është hartuar në përputhje me Parimet Udhëzuese të Kombeve të Bashkuara për Biznesin dhe të Drejtat e Njeriut[9], duke e respektuar atë në çdo rresht të saj. Por, një fakt mjaft interesant është se në një pjesë të kësaj kontrate, kompania shprehet që nuk mban asnjë përgjegjësi në rast të keqpërdorimit të teknologjisë nga qeveritë blerëse (kjo mund të interpretohet si një boshllëk i qëllimshëm ligjor që klientët e saj të abuzojnë gjerësisht me këtë program mbikqyrjeje).

Megjithatë, në një intervistë të kohëve të fundit, vetë CEO-ja i Kompanisë NSO ka deklaruar se, "Ne vetëm ia shesim produktet tona qeverive dhe nuk kemi asnjë mjet për të kontrolluar se çfarë këto qeveri bëjnë me to…. Nëse këto qeveri e keqpërdorin sistemin, ne mund të gjejmë një mënyrë për të hetuar në lidhje me këtë fakt.Në përfundim të hetimit, nëse vërtetohet se, në fakt, ka raste të keqpërdorimit të tyre, ne mund të mbyllim programin që ata përdorin. E kemi bërë më përpara këtë gjë dhe do të vazhdojmë ta bëjmë. Por ne nuk mund të fajësohemi për keqpërdorimin në vetvete që bën qeveria."[10]

Në përputhje me sa më lart, Kompania NSO publikoi edhe një raport transparence[11], ku fakton se ka mbyllur të paktën dy kontrata (duke humbur një vlerë prej mbi 300 milion dollarësh amerikanë) me shtete që dukshëm shkelnin të drejtat e njeriut. Disa qeveri të tjera janë në hetim e sipër.

Ekpertët e informaconit mbi sigurinë në survejim janë të bindur që "Pegasus" nuk përdoret për të mbikëqyrur njerëzit e thjeshtë, por për të survejuar individë specifikë, aktivitetet e të cilëve përbëjnë interes të veçantë për ata që e kontrollojnë këtë teknologji.Çdo licensë e "Pegasus" kushton miliona dollarë amerikanë nësë blihet, ose rreth 100.000 dollarë amerikanë nëse merret me qera mujore, rrjedhimisht mbikëqyrja bëhet vetëm ndaj personave që kanë informacione të vlefshme. Personat që janë potencialë për survejim janë:

- Liderët e politikës së një shteti.

9 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

10 https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-"Pegasus"-project-hacking-allegations/?sh=6bc6d157472d

11 https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

- Të emigruarit e profilit të lartë (për shembull, numri i telefonit i Pavel Durov, CEO-ja i Telegram-it, dyshohet se është shënjestuar nga Emiratet e Bashkuara[12] pasi ai u zhvendos të jetonte atje).
- Persona që kanë informacion të vlefshëm strategjik apo ushtarak.
- Gazetarët dhe aktivistët e të drejtave të njeriut.
- Shkencëtarët e kompanive të një profili të lartë strategjik (për shembull zhvilluesit e armatimeve nukleare).
- Kriminelët (kryesisht terroristë dhe pedofilë).

Në 18 korrik të vitit 2021 qarkulloi një lajm jo pak tronditës rreth përdorimit të teknologjisë "Pegasus". Sipas këtij lajmi, kjo pajisje survejuese e gradës ushtarake po përdorej për të hakeruar telefonat e mbi 50 mijë personave që prej vitit 2016, duke treguar edhe ditën dhe orën kur këto pajisje ishin infektuar. Për herë të parë teknicienët e skuadrës kibernetike të *Amnesty International* publikuan një listë të gjatë përgjimesh masive nga një qeveri e caktuar të personaliteteve të ndryshme, jo vetëm të shtetit në krye të së cilës ajo qëndron, por edhe të shteteve të tjera të huaja. Në fund ky publikim, i quajtur "Projekti Pegasus", doli në përfundimin se përgjoheshin persona të të paktën 45 shtetësive të ndryshme, të cilët ishin shënjestuar nga të paktën 10 qeveri të ndryshme që kishin blerë licensën nga NSO-ja.

Nga kjo listë, është vërtetuar se të paktën 1000[13] numra telefoni përdoreshin nga anëtarë të familjeve mbretërore arabe, nga këshilltarë të Dalai Lamës, nga diplomatë, nga oficerë sigurie dhe ushtrie, nga 65 pronarë biznesesh, 85 aktivistë të të drejtave të njeriut, 189 gazetarë dhe më shumë se 600 politikanë (mes tyre edhe presidenti francez Makron, Mbreti Mohamed VI i Marokut, presidentët e Irakut dhe të Afrikës së Jugut, disa kryetarë qeverish, ministra të kabinetit). Shumica e personave të përgjuar ishin me shtetësi meksikane.

1.3 Kush nuk gjendet në listën famëkeqe të këtyre përgjimeve?

Deri më tani, asnjë kompani apo numër telefoni amerikan nuk është shënjestruar nga "Pegasus".Edhe pse rreth një duzinë amerikanësh, të cilët

12 https://www.cpomagazine.com/cyber-security/data-leak-reveals-"Pegasus"-spyware-found-in-use-unlawfully-in-20-countries-with-capability-to-break-current-iphone-security/#:~:text=The%20leaked%20data%20led%20to,United%20Arab%20

13 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-"Pegasus"-cellphones/

punonin matanë oqeanit, janë zbuluar në këtë listë, vetëm në njërin prej rasteve telefoni ishte rregjistruar në një rrjet celular të huaj. Duke qenë se shitja e licensës "Pegasus" tek qeveritë e huaja duhet të miratohet nga Ministria e Mbrojtjes, kjo politikë mospërgjimi reflekton frymën e përgjithshme për të ruajtur një marrëdhënie të mirë me aleatin më të madh strategjik që Izraeli ka. Nga ana tjetër, Kompania NSO mund të ketë patur frikë që Shtetet e Bashkuara të Amerikës do mund ta zbulonin këtë teknologji përgjimi dhe të binin në gjurmët e vetë kompanisë[14].

Në të gjithë këtë histori ka dy aspekte të paqarta:

- Nga njëra anë, *Amnesty International* nuk e tregon burimin se nga e ka marrë, apo ku është bazuar për të "krijuar" këtë listë. Vetë ajo ka deklaruar se këto të dhëna nuk konfirmojnë personat e shënjestruar, por vetëm "i sugjerojnë" ato. Madje, në shumë raste as nuk mund të konfirmohet nëse ky telefon është infektuar realisht me "Pegasus", apo thjesht është tentuar të infektohet me këtë virus[15]. Për këtë arsye Laboratori i Sigurisë i *Amnesty International* ekzaminoi 67 smartphone që dyshoheshin se përgjoheshin. Nga këta, 23 prej tyre ishin infektuar me sukses me "Pegasus", ndërsa për 14 syresh u gjetën shenja të tentimit të infektimit.Rezultatet për 30 telefonat e ngelur nuk ishin të qarta pasi në këto raste telefonat ishin zëvendësuar.Nga këto telefona, 15 ishin të llojit Android[16].

- Nga ana tjetër, një nga drejtuesit[17] e Kompanisë NSO ngul këmbë që ky raportim nuk është i vërtetë sepse nuk ekziston asnjë server që përmban një listë me emrat e të gjithë personave që përgjohen. Sipas tij, shifra prej 50 mijë personash është anormale, kjo sepse numri mesatar që një licensë "Pegasus" mund të shënjestrojë është rreth 100 dhe se deri tani kompania e ka shitur në rreth 40 apo 45 shtete teknologjinë e saj[18].

Meksika ka qenë klienti i parë ndërkombëtar i NSO-së që ka blerë licensën "Pegasus", pothuajse një vit pasi teknologjia ishte prodhuar. Sot, përdorimi i "Pegasus" është faktuar në 45 shtete të ndryshme të botës: Algjeri, Bahrain, Bangladesh, Brazil, Kanada, Bregun e Fildishtë, Egjipt, Francë, Greqi, Indi, Irak, Israel, Jordani, Kazakistan, Kenia, Kuvait, Kirgistan, Letoni, Lebanon,

14 https://www.vice.com/en/article/wnxpjm/nso-group-new-big-player-in-government-spyware

15 https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-"Pegasus"-project-hacking-allegations/?sh=6bc6d157472d

16 https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-"Pegasus"/

17 https://www.youtube.com/watch?v=YkiAnBIoGRg

18 https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-"Pegasus"-project-hacking-allegations/?sh=6bc6d157472d

Libi, Meksikë, Marok, Holandë, Oman, Pakistan, Palestinë, Poloni, Katar, Ruandë, Arabi Saudite, Singapor, Afrikë të Jugut, Zvicër, Taxhikistan, Tajlandë, Togo, Tunizi, Turqi, Emiratet e Bashkuara Arabe, Ugandë, Mbretëri të Bashkuar, Shtetet e Bashkuara të Amerikës, Uzbekistan, Jemen dhe Zambi. Sigurisht këto gjetje nuk janë përfundimtare pasi bazohen në nivelin e venndodhjes gjeografike të serverave DNS[19], prandaj faktorë si VPN[20] dhe lëvizjet e satelitëve që shpërndajnë internetin mund të çojnë në pasaktësi.Të paktën 10 nga këto shtete përgjojnë edhe jashtë shtetit të tyre.Ato dyshohet se janë Azerbajxhani, Bahraini, Hungaria, India, Kazakistani, Meksika, Maroku, Ruanda, Arabia Saudite dhe Emiratet e Bashkuara Arabe[21].

Kreu II

2.1 Si mund të infektohet një telefon i teknologjisë së fundit (smartphone) nga "Pegasus"?

Në kohët e sotme ne të gjithë komunikojmë me miqtë dhe familjarët nëpërmjet aplikacioneve të mesazheve direkte, dhe në disa raste edhe nëpërmjet postës elektronike. Nëse jeni të rregullt në kontrollin e folderit të "Inbox"-it të postës suaj elektronike (duke qëndruar të përditësuar me komunikimet më të fundit), me siguri e keni vënë re edhe një folder tjetër aty të emërtuar "Spam", nëpërmjet të cilit shpërndarësit e intenetit si, Gmail-i, Outlook-u apoYahoo-jafiltrojnë për llogarinë tuaj mesazhet në dukje të pasigurta. Një ndër mënyrat infektuese që përdor "Pegasus" është duke gjetur një formë që këto mesazhe të anashkalojnë filtrin "Spam" dhe të përfundojnë në folderin "Inbox" të postës suaj elektronike. Kësisoj ato do të duken si email-e të zakonshme, të cilat supozohet të jenë të sigurta. Këto quhen "sulme me një klikim" dhe "Pegasus" aktivizohet kur përdoruesi klikon mbi linkun e dërguar.Me hapjen e tij, "Pegasus" përfton akses të plotë në smartphone-in e përdoruesit, qoftë ai një Android, apo një Iphone. Sa më lart nuk bëhet vetëm nëpërmjet e-mail-it, por virusi mund të transmetohet edhe nëpërmjet një mesazhi Sms, Whatsapp-i, Instagram-i, apo edhe përmes atyre që mendohen se janë aplikacionet më të sigurta të komunikimit si Signal dhe Telegram. Marrja e të dhenave mundësohet përmes asaj që quhet "dobësia e ditës zero – zero day vulnerability" ose siç njihen ndryshe, viruset në procesin e krijimit të softuerit. Këto viruse lindin që në çastin e krijimit të

19 Domain Name System

20 Virtual Private Network

21 https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-"Pegasus"-spyware-to-operations-in-45-countries/

teknologjisë software, të nevojshme për funksionimin e çdo smartphone-i, e si rrjedhim, nuk mund të indentifikohen dhe eleminohen nga programet e zakonshme anti-virus. Viruset e ditës zero (zero day bugs) sapo janë zbuluar nga disa organizata të pavarura të sigurisë dhe kërkimeve në intenet. Kur gjenden, këto viruse duhet të raportohen pa humbur kohë te pronarët e sistemeve funksionuese, Google (për Android), apo Apple (për iOS).

Këto viruse ndahen në: viruse të zakonshme (common bugs) që mund të eliminohen nga teknikët e sigurisë që punojnë në Google dhe në Apple, dhe në viruse të ditës zero (zero day bugs), të cilat nuk mund të eliminohen, ndryshe do të shkaktonin një mosfunksionim thelbësor të sistemit operativ të smartphone-it.

Edhe pse kompanitë mundohen t'i eliminojne ato, viruset "common bugs" zakonisht përfundojnë në "dark web"[22] (rrjeti i errët) ku hakerat kanë mundësi të krijojnë një "link"[23] që përmban një kod dashakeq që thyen sigurinë e telefonit. Më pas, ky link u dërgohet përdoruesve të thjeshtë me e-mail apo me mesazh. Kjo është mënyra se si hakerat "ordinerë" infektojnë smartphone-at me viruse, të cilat më pas u mundësojnë thyerjen e privatësisë.

Frymëzuar nga kjo mënyrë hakerimi, vitet e fundit "Pegasus" e ka përsosur mënyrën e infektimit të telefonit nëpërmjet atij që quhet sulmi me zero klikim (zero click attack) duke përdorur viruset e ditës zero – thelbësore për funksionimin e telefonave (viruse që nëse do të shkatërroheshin, do shkatonin mosfunksionim të vetë telefonit). Nëpërmjet virusit thelbësor dërgohet një mesazh në një ndër aplikacionet e komunikimit që përdoren më së shumti (whatsapp, email, iMessage, sms, etj.,….), apo dërgohet një telefonatë anonime (No user ID) në telefonin e përdoruesit. Nuk ka nevojë që këto mesazhe të klikohen apo që telefonata të përgjigjet. "Pegasus" aktivizohet sapo mesazhi apo telefonata shkon në smartphone, prandaj edhe quhen sulme me zero klikim – përdoruesit nuk i duhet të klikojë mbi këto njoftime. Jo vetëm kaq, por me t'u aktivizuar virusi, këto njoftime vetë-fshihen.Kjo bën që përdoruesi i zakonshëm ta ketë të pamundur që ta kuptojë se po mbikëqyret nëpërmjet smartphone-it të tij.

Shkarkimi dhe instalimi i programit të spiunimit "Pegasus" në telefon është i padukshëm dhe i pagjurmueshëm – nuk gjendet asnjë folder në telefon që të tregojë praninë e tij. Madje, edhe ngadalësimi i funksionimit të telefonave që e bartin këtë virus pas një apo dy vitesh, i atribuohet konsumimit të vetë

22 https://pcworld.al/dark-web-per-shume-perdorues-eshte-ana-e-padukshme-e-internetit/

23 Link-u është një kanal komunikimi që lidh dy ose më shumë pajisje me qëllimin e shpërndarjes së informacionit

softueri-t të telefonit. Askujt nuk i shkon në mendje të kontrollojë me detaje nëse këtë ngadalësim po e shkakton ndonjë virus, apo diçka tjetër.

2.2 Sistemi i të dhënave ku "Pegasus" ka akses.

Të dhënat që përfton "Pegasus":

[24]

Informacion sensitiv:

- Përmes sensorëve të smartphone-it shkrepen fotografi, si nëpërmjet kamerës kryesore, ashtu edhe nëpërmjet asaj dytësore.
- Shkrepen fotografi dhe xhirohen video të ekranit.
- Xhirohen video dhe regjistrohen audio në çdo moment, jo vetëm kur viktimat25 po komunikojnë nëpërmjet telefonit, por edhe nëse pajisja nuk po përdoret nga përdoruesi. Në këtë rast "Pegasus" sigurohet që telefoni nuk po përdoret dhe dërgon një telefonatë të padukshme (pa zile dhe pa figurë). Përmes kësaj telefonate aktivizohet mikrofoni dhe fillon regjistrimi. Nëse telefoni fillon të përdoret, telefonata automatikisht shkëputet, sigurisht pa lënë asnjë gjurmë.
- Dëgjohen dhe regjistrohen mesazhet e shkruara, si edhe bisedat e përdoruesit, jo vetëm duke përdorur linjën normale telefonike, por edhe çdo aplikacion tjetër, madje edhe ato që mendohen se nuk mund të përgjohen (Telegram, Whatsapp, Messenger, Signal, Viber, Wire, etj.,.).

24 https://www.vice.com/en/article/wnxpjm/nso-group-new-big-player-in-government-spyware

25 Personat, smartphone-t e të cilëve janë infektuar me virusin "Pegasus"

- Shkarkohet, ruhet, ndryshohet dhe regjistrohet çdo dokument që gjendet në dosjet e telefonit, si edhe nëpër adresat elektronike.
- Monitorohet posta elektronike.
- Kontrollohet lista e kontakteve – nga këtu mund të gjendet numri i telefonit i një personi të tretë me interes, i cili më pas mund të përdoret për të instaluar "Pegasus" edhe te pajisja e tij.
- Aksesohen të dhënat bankare (nëse përdoruesi në telefonin e tij ka instaluar një aplikacion e-banking, ose nëse ai e përdor telefonin për blerje online).
- Kontrollohet vendndodhja në kohë reale – nëse përdorusesi e ka GPS-në e çaktivizuar, "Pegasus" e aktivizon atë vetëm sa për lokalizimin e vendndodhjes së tij dhe menjëherë e fik. Nëse telefoni nuk ka GPS, vendndodhja gjendet përmes numrit IMEI të telefonit.
- Ka akses pa limit në të gjitha rrjetet sociale që përdoruesi i telefonit përdor.
- Mundëson vendosjen e lajmërimeve paraprake për veprime në kohë reale – për shembull, "Pegasus" lajmëron nëse personi që po mbikëqyret hyn apo del nga një ambient i caktuar; nëse ai po takohet me persona të tjerë nën mbikëqyrje; nëse personi telefonon apo telefonohet, apo dergon/merr ndonjë mesazh drejt/nga një numër specifik; nëse telefonata apo mesazhi përmban një fjalë-kod të caktuar, të vendosur paraprakisht nga survejuesi.

Informacion i parëndësishëm:

- Emri dhe fjalëkalimi i lidhjes wi-fi që përdoruesi ka në telefon.
- Cila ka qenë blerja e fundit që përdoruesi ka bërë përmes telefonit.
- Në cilin orar e vendos përdoruesi zilen e zgjimit në mëngjes.
- Rutina e tij e palestrës.
- Cilësimet e celularit të tij.
- Histroriku i kërkimeve të tij në internet.
- Lista e tij e punëve për t'u bërë.
- Regjistimet kalendarike, etj…

Këto të dhëna transmetohen përmes një procesi të automatizuar në

serverat qendrorë ku organiazata spiune "mëmë" proceson informacionin në nivel qelizor. Më pas ky informacion transferohet i dekriptuar në serverin lokal (kompjuterin) e personit të interesuar që ka licensën e përdorimit. Ky proces përfundon në milisekonda. Pra, monitorimi i telefonit të personit të shënjestruar bëhet në kohë reale.

Transmetimi i të dhënave ndalon automatikisht nëse bateria e aparatit të tij celular është në nivel të ulët, ose kur personi i shënjestruar e ka telefonin e tij në modalitetin Roaming.Në këto raste, kur transmetimi në kohë reale është i pamundur, "Pegasus" i ruan të dhënat e mbledhura në një program te veçantë në telefon, plotësisht i fshehtë dhe i enkriptuar, i programuar për të mos zënë më shumë se 5% të memories së lirë të telefonit.Këto të dhëna bëhen të aksesueshme në një moment të dytë, kur bateria e telefonit është e karikuar, ose kur përdoruesi nuk e ka më telefonin e tij në modalitetin Roaming. Në raste të jashtëzakonshme, kur transferimi është i pamundur përmes kanaleve të sigurta, një virus mund të mbledhë të dhënat urgjente përmes SMS-ve, por NSO-ja paralajmëron se në raste të tilla "Pegasus" mund të zbulohet nga përdoruesi për shkak të faturës së lartë të telefonit.

2.3 Funksioni i mekanizimit të vetëshkatërrimit.

"Pegasus" shoqërohet edhe me një mekanizëm vetëshkatërrimi.

- Ai mund të aktivizohet në çdo moment nga mbikëqyrësi, duke mos lënë asnjë gjurmë që të mund të vërtetojë se në një çast të caktuar tek ai aparat telefonik ka qenë i instaluar "Pegasus".
- Gjithashtu, mekanizmi i vetëshkatërrimit aktivizohet automatikisht, nëse ekziston një rrezik potencial për ekspozim – kjo ndodh nëse "Pegasus" nuk komunikon me serverin nga telefoni i infektuar për 60 ditë me radhë, ose per çfaredo afati tjeter, i vendosur manualisht nga mbikqyrësi.
- Skenari i tretë i aktivizimit të mekanizmit të vetëshkatërrimit ndodh kur viktima futet në Shtetet e Bashkuara të Amerikës. Kjo sepse Kompania NSO e ka projektuar "Pegasus" për të mos mbikëqyrur numrat amerikanë. Rrjedhimisht, sapo rrjetet amerikane të komunikimit vendosen në telefonin e të mbikëqyrurit, "Pegasus" automatikisht vetëshkatërrohet.

Teknologjia komplekse e spiunazhit ka akses deri në folderat rrënjë që ndodhen në telefonat tanë.Në këto foldera gjendet informacioni që është

thelbësor për funksionimin e sistemeve Android dhe iOS. Rrjedhja e këtij informacioni kaq privat është një goditje e rendë poshtë brezit, jo vetëm për sigurinë, por edhe për privatësinë e individit. Për këtë arsye, në Nëntor të vitit 2021, "Pegasus" u vendos në listën e zezë të Shteteve të Bashkuara të Amerikës nga administrata e Presidentit Bajden, duke ndaluar kësisoj çdo perdorim apo studim të kësaj teknologjie në territorin amerikan.

Kreu III

3.1 Si të zbuloni nëse "Pegasus" ndodhet në smartpone-in tuaj?

Laboratori i Sigurisë i *Amnesty International* ka zhvilluar në Korrik të vitit 2021 një program për dekriptimin e përmbajtjes së telefonit dhe këqyrjen e tij për të evidentuar praninë e çdo virusi, përfshirë "Pegasus". Programi quhet *Mobile Verification Tool* (MVT – Mjeti per Verifikimin e Smartphone) dhe funksionon për çdo aparat smartphone.Momentalisht MVT-ja është në proces zhvillimi dhe testimi si aplikacion në Playstore[26] dhe Appstore[27] për akses nga përdoruesi i zakonshëm.Rrjedhimisht testimi i MVT-së bëhet vetëm nga persona të specializuar dhe të informuar rreth teknologjisë kompjuterike. Shkurtimisht, përdorimi i MVT-së për aparatet telefonike Iphone realizohet vetëm në kompjuterat MAC[28], kurse për aparatet telefonike Android ai realizohet në sistemin LINUX[29]. Pasi bëhet një backup i enkriptuar i aparatit smartphone, instalohet MVT-ja duke e kopjuar nga faqja zyrtare e *Amnesty International*dhe ngjitur në faqen command të kompjuterit. Më pas ndiqen hapat teknike të rekomanduara në dokumentacionin e vënë në dispozicion nga *Amnesty International*.Pasi instalohet, MVT-ja skanon të gjitha të dhënat e aparatit smartphone, tashmë të dekriptuara, dhe me paralajmërime në ngjyrë të kuqe (warnings) tregon praninë e çdo virusi, përfshirë edhe "Pegasus". Programi ka vetëm fuqi zbuluese, por jo ndaluese. Mënyra e vetme e njohur për heqjen e këtij të fundit thuhet se është duke bërë një rikthim në gjendje fillestare (fabrike) të telefonit. Megjithatë mund të themi se edhe ky veprim nuk jep garanci të plotë dhe absolute për largimin e infektimit apo riinfektim në të ardhmen. Zakonisht, personat që kanë zbuluar se po monitorohen me "Pegasus", kanë zgjedhur t'i zëvendësojnë aparatet e tyre smartphone me të

26 Dyqani i aplikacioneve per iPhone

27 Dyqani i aplikacioneve per Android

28 Familja e kompjuterave prodhuar nga Apple

29 https://www.techtarget.com/searchdatacenter/definition/Linux-operating-system

rinj dhe njëkohësisht kanë blerë numra të rinj telefoni, jo më në emrin e tyre.

Konkluzione dhe rekomandime

Mund të themi me bindje se "Pegasus" ka anët e veta pozitive, ato negative dhe "të errëta".

Anët pozitive:

Konkretisht, vitet e fundit "Pegasus" është përdorur[30] me sukses gjerësisht për:

- Parandalimin e sulmeve terroriste, duke përfshirë përdorimin e armëve në vende publike, bombat nëpër makina, bombarduesit vetëvrasës (kamikazë) në mjetet e transportit publik ose në parqe publike, markete, evente koncertesh, arenash sportive dhe në shumë vende të tjera publike.
- Ndalimin e pedofilëve, organizatave të trafikimit seksual dhe të lëndëve narkotike, dhe operacioneve të ndryshme për pastrimin e parave.
- Gjetjen dhe shpëtimin e fëmijëve të rrëmbyer.
- Në gjetjen e të mbijetuarve të bllokuar nën rrënojat e ndërtesave të rëna në rastet e fenomeneve shkatërruese natyrore, por edhe në rastet e ndërtesave të ngritura në mënyrë jo të sigurt, në bashkëpunim edhe me skuadrat e emergjencës.

Anët negative:

Kjo pajisje survejuese dyshohet se po përdoret për të hakeruar telefonat e mbi 50 mijë personave që prej vitit 2016.Hetimi gazetaresk Projekti "Pegasus"[31] doli në përfundimin se po përgjoheshin persona të të paktën 45 shtetesive të ndryshme, të cilët ishin shënjestuar nga të paktën 10 qeveri të ndryshme që e kishin blerë licensën nga NSO-ja. Nga kjo listë, është vërtetuar se rreth 1000[32] numra telefoni përdoreshin nga anëtarë të familjeve mbretërore arabe, nga keshilltarë të Dalai Lamës, nga diplomatë, nga oficera sigurie dhe ushtrie, nga 65 drejtues biznesesh, 85 aktivistë të të drejtave të njeriut, 189 gazetarë, dhe më shumë se 600 politikanë (mes tyre edhe

30 https://www.nsogroup.com/about-us/

31 https://en.wikipedia.org/wiki/Pegasus_Project_(investigation)

32 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-"Pegasus"-cellphones/

presidenti francez Makron). Para pak muajsh madje u hodhën dyshime se policia e Izraelit po përdorte "Pegasus" për të përgjuar qytetarët pa një mandat gjyqësor[33].Momentalisht, çeshtja po hetohet, dhe nga analizat paraprake këto pretendime nuk rezultojnë të vërteta.

Impakti mbi Të drejtat dhe liritë themelore të njeriut:

Liritë dhe të drejtat themelore të njeriut janë të lidhura dhe forcojnë njëra-tjetrën. Prandaj, teknologjitë e mbikqyrjes elektronike kanë një efekt shkatërrues jo vetëm mbi to, por edhe mbi të drejtën për privatësi dhe atë të fjalës së lirë.

- Për shembull, edhe e drejta e shëndetit mund të dëmtohet nga praktikat e survejimit digjital pasi njerëzit, nga frika e kompromentimit të konfidencialitetit, mund të tërhiqen nga shpërndarja elektronike e të dhënave të shëndetit të tyre me mjekun specialist të familjes.
- E drejta e fesë gjithashtu mund të preket, sidomos nëse përgjohen dhe vidhen komunikimet private konfidenciale me shërbyesit fetarë.
- Vetë individët mund të tërhiqen nga zbatimi i të drejtës së tyre për të formuar organizata jofitimprurëse me karakter politik, filozofik, tregëtar apo fetar, duke patur frikë për shëndetin dhe jetën,jo vetëm për vete por edhe për familjarët e tyre.
- Përgjimi mbi një masë të madhe njerëzish krijon një klimë vetë-censuruese për njerëzit. Frika se çdo veprim i tyre është nën kontroll, mund të bëjë qëatatë tërhiqenjo vetëm nga jeta sociale, por edhe nga publikimet online në platformat e tyre pesonale, duke çuar në këtë mënyrë në një izolim social.
- Edhe të afërmit apo miqtë e personave të përgjuar mund të largohen nga çdo ndërveprim me "viktimat" nga frika se mos edhe ata mund të vendosen nën përgjim.
- Por,fakti mëshqetësues është se kjo ndërhyrje e pashoqe në jetën private, mund ta rrezikojë integritetin fizik dhe mendor të personit, duke e çuar atë deri në kryerjen e veprimeve që mund të rrezikojnë seriozisht jetën dhe shëndetin e tij.

Organizatat e shoqërisë civile gjithmonë e më shumë po kërkojnë

33 https://appleinsider.com/articles/22/01/18/israeli-police-use-nso-groups-"Pegasus"-to-spy-on-citizens-without-a-warrant

vendosjen e një moratoriumi në shitjen, transferimin dhe përdorimin e "Pegasus" deri sa të garantohet që ai do të jetë në përputhje me strandartet dhe konventat ndërkombëtare të të drejtave të njeriut. Këto organizata u kërkojnë urgjentisht shteteve që të implementojnë një legjislacion që garanton siguri ndaj shklejeve të të drejtave të njeriut, abuzimeve me survejimin digjital, dhe sidomos të garantojnë dënueshmëri për ata përgjues që shkelin këto të drejta.

Anët e errëta:

- Një rrjedhje informacioni në hetimin ndaj "Pegasus" tregoi se Maroku kishte vënë në përgjim më shumë se 200 shtetas spanjollë34 nëpërmjet "Pegasus". Megjithatë, Maroku e mohoi me ngulm këtë deklaratë duke treguar që nuk ekziston asnjë metode verifikimi që ata janë në posedim të kësaj teknologjie.
- Nga një kërkim i kryer nga Universiteti i Torontos rezultoi se të paktën 65 persona të lidhur me Lëvizjen e Pavarsisë Katalanase ishin vënë në përgjim me "Pegasus" nga qeveria Spanjolle përgjatë viteve 2017-202035.
- Pasi "Pegasus" u ble nga Emiratet e Bashkuara Arabe, një rrjedhje e brendshme informacioni tregoi se teknologjia po përdorej për të përgjuar Ahmed Mansurin, aktivistin më të njohur dhe të respektuar të të drejtave të njeriut në Emiratet e Bashkuara Arabe. Brenda një viti ai u burgos36.
- Ka dyshime se "Pegasus" është përdorur nga Dubai për të përgjuar persona me interes në Mbretërinë e Bashkuar37, sigurisht pa mandate gjyqësore.
- Në Meksikë kanë qarkulluar në media dokumenta që vërtetojnë përdorimin e "Pegasus" ndaj një grupi ekspertësh ndërkombëtar, të cilët po merreshin me shqyrtimin e çështjes së 43 studentëve, të cilët u

34 https://www.theguardian.com/world/2022/may/03/over-200-spanish-mobile-numbers-possible-targets-"Pegasus"-spyware

35 https://www.theguardian.com/world/2022/may/15/use-of-"Pegasus"-spyware-on-spains-politicians-causing-crisis-of-democracy

36 https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

37 https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

zhdukën pas një përplasjeje me policinë vendase38.

- Çështje të shumta gjyqësore janë ngritur kundër Kompanisë NSO për teknologjinë "Pegasus", por në asnjërën prej këtyre çështjeve nuk është arritur të vërtetohen shkelje të tilla nga themeluesit. Çdo survejim i hetuar është vërtetuar se është kryer me mandat gjyqësor, si dhe çdo license e shitur apo e dhënë me qera është dokumentuar përmes verifikimeve me "Vetting" të instancave shtetërore kërkuese dhe e blinduar me kontrata qeveritare. Madje, Kompania NSO e ndalon shitjen e licensës qoftë te individët fizikë, qoftë te kompanitë private. Kjo nënkupton që, nëse do të ketë abuzim, ky do të jetë domosdoshmërisht në nivel shtetëror, ku NSO-ja nuk mund të ushtrojë kontroll.Për më tepër, përdorimi në masë i "Pegasus", jo vetëm që do të sillte mbingarkim dhe mosfunksionim të sistemit, por është edhe i pamundur për t'u përballuar ekonomikisht pasi Kompania NSO kërkon të paguhet në nivel përgjimi individual. Pra, ajo kërkon pagesën e një tarife të caktuar për çdo person, të cilit do t'i instalohet virusi.

Disa rekomandime në lidhje me sigurinë e telefonit

Masat paraprake që mund të merren për ta mbajtur aparatin smartphone të sigurt:

- Përditësimi i vazhdueshëm i sistemit operativ, si edhe i të gjitha aplikacioneve individuale zakonisht viruset që hakerat përdorin zbulohen nga teknikët e Google dhe Apple, të cilët menjëherë dërgojnë për shkarkim zgjidhjen përkatëse për përforcimin e sigurisë së telefonit.
- Shmangia e shkarkimit të aplikacioneve Android jo nëpërmjet Playstore-it, por duke përdorur file si dot.apl. Këto aplikacione nuk kanë filtra sigurie duke mundësuar futjen e viruseve që cënojnë privatësinë tuaj.
- Mos-hapja e mesazheve e-mail nga persona të panjohur. Edhe nëse ato hapen, nuk duhet klikuar mbi linkun që zakonisht i shoqëron këto mesazhe.
- Vendosja e fjalëkalimeve të vështira, dhe domosdoshmërisht aktivizimi i autentifikimit me dy faktorë.
- Nëse është e mundur komunikimi me mesazhe të bëhet në modalitetin

38 https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-"Pegasus"-spyware.html

privat – të mundësohet vetëshkatërrimi i tyre pak sekonda pasi janë lexuar nga palët.

- Mosklikimi mbi domaine të panjohura. Zakonisht mënyra më e sigurt për të lundruar në internet është duke klikuar në faqe web, të cilat fillojnë me https://.

Referenca:

Faqe web e Grupit NSO, https://www.nsogroup.com/

Faqe web e Grupit Mediatik Vice,https://www.vice.com/en

Faqe web e Kombeve të Bashkuara, https://www.un.org/en/

Faqe web e Forbes, https://www.forbes.com/?sh=12d0eecc2254

Faqe web e CPO Magazine,https://www.cpomagazine.com/

Faqe web e The Washington Post,https://www.washingtonpost.com/

Faqe web e Amnesty International, https://www.amnesty.org/en/

Faqe web e Citizenlab, Universiteti i Torontos, Kanada, https://citizenlab.ca/

Faqe web e Këshillit të Europës, https://www.coe.int/en/web/portal

1. Faqe web e The Guardian, https://www.theguardian.com/international

2. Faqe web e Apple Insider, https://appleinsider.com/

Faqe web e New York Times,https://www.nytimes.com/

Konventa Evropiane e të Drejtave të Njeriut https://www.echr.coe.int/documents/convention_sqi.pdf

NDRYSHIMET E LEGJISLACIONIT TË BE-SË MBI PARANDALIMIN E PASTRIMIT TË PARAVE LIDHUR ME PORTOFOLET ANONIME TË KRIPTO-MONEDHAVE

PROF. ASOC. EVISA KAMBELLARI ESQ.

Avokate, SHBA

ekambellari@aol.com

PROF. ASOC. ENGJELL LIKMETA

Profesor, Departmenti i së Drejtës Penale, Universiteti i Tiranës

engjell.likmeta@fdut.edu.al

Abstrakt

Punimi synon të analizojë rregullat e reja të BE-së lidhur me forcimin e gjurmueshmërisë të kripto-monedhave në një përpjekje për të forcuar stabilitetin financiar dhe luftën kundër pastrimit të parave të ardhura nga aktiviteti kriminal.

Direktiva (BE) 2018/843 kërkon prej shteteve anëtare që të sigurojnë që ofruesit e shërbimeve të shkëmbimit të monedhave virtuale[1] me para letre, ofruesit e shërbimeve të ruajtjes së portofolit[2], zyrat e shkëmbimit të

1 Neni 3 i Direktivës 2018/843 përkufizon monedhat virtuale si "një përfaqësim dixhital të vlerës që nuk është emetuar ose garantuar nga një bankë qendrore ose një autoritet publik, nuk është domosdoshmërisht e lidhur me një monedhë të krijuar ligjërisht dhe nuk ka një status ligjor të monedhës ose parasë, por është pranuar nga personat fizikë ose personat juridikë si mjet këmbimi dhe që mund të transferohet, ruhet dhe tregtohet në mënyrë elektronike".

2 Ofruesi i shërbimeve të kuletës është një subjekt që ofron shërbime për të mbrojtur çelësat privatë kriptografikë në emër të klientëve të tij, për të mbajtur, ruajtur dhe transferuar monedha

monedhave dhe arkëtimit të çeqeve, të jenë të licensuara ose të regjistruara.

Përdorimi i kripto-aseteve ka hapur një botë të re mundësish investimi, operimi, dhe transaksionesh. Në të njëjtën kohë, aspekti virtual dhe anonim i këtyre operacioneve ka krijuar një mjedis joshës për pastrimin e parave të ardhura nga aktiviteti kriminal.

Në këtë punim synojmë të prezantojmë se si rregullat e reja të BE-së përpiqen të ndalojnë anonimitetin e lidhur me transfertat e kripto-aseteve dhe cilat janë efektet e këtyre kufizimeve.

Hyrje

Në përgjigje të luftës kundër pastrimit të parave dhe financimit të terrorizmit, Bashkimi Evropian ka miratuar një sërë Direktivash në dekadën e fundit. Direktiva e fundit është Direktiva (BE) 2018/843, e njohur ndryshe si direktiva AML 5, e cila hyri në fuqi më 10.01.2020.

Direktiva e re synon të zgjerojë më tej rregullimin e vendosur nga Direktiva e meparshme e BE-së (2015/849) "Mbi parandalimin e përdorimit të sistemeve financiare për qëllime të pastrimit të parave".

Direktiva 2018/843/BE forcon strukturën aktuale të luftës kundër pastrimit të parave dhe financimit të terrorizmit në disa mënyra: duke rritur transparencën lidhur me pronësinë e kompanive përfituese, duke rritur bashkëpunimin dhe ndarjen e informacionit midis autoriteteve të mbikëqyrjes financiare, nëpërmjet vendosjes së rregullave më të forta për transaksionet me klientë nga vende me risk të botës së tretë, nëpërmjet kufizimit të përdorimit anonim të monedhave virtuale, si dhe zgjerimit të fushës së veprimit të sektorëve dhe entiteteve mbi të cilat rëndojnë detyrimet që rrjedhin prej direktivës.

Një nga kërkesat kryesore të kësaj direktive është që shtetet anëtare duhet të mbajnë një regjistër qendror të përfituesit ose pronarëve të firmave, si dhe për administruesit brenda juridiksionit të tyre, të mbajnë informacion të azhornuar të pronësisë së përfituesve të trusteve të tyre.

---

virtuale. Shih më sipër, neni 3 i Direktivës.

1. Rreziqet e përdorimit të kripto-monedhave në aktivitete të paligjshme

Anonimiteti që shoqëron modalitetet e pagesës nëpërmjet kripto-monedhave favorizon përdorimin e tyre në një sërë aktivitetesh të paligjshme si pastrimi i produkteve të veprës penale, financimi i aktiviteteve terroriste, evazioni fiskal, si dhe vepra penale që cenojnë interesat financiare të individëve ose subjekteve juridike.[3]

Pavarësisht përpjekjeve të ligjvënësve për të rritur kërkesat e raportimit të transaksioneve që kryhen me anë të kripto-monedhave, niveli i monitormit dhe gjurmueshmërisë të këtyre transaksioneve mbetet relativisht i ulët krahasuar me transaksionet e kryera nëpërmjet rrjeteve të institucioneve konvencionale finaciare. Për këtë arsye, të tilla transaksione shfrytëzohen nga subjektet kriminale për pastrimin e parave të ardhura nga aktivitetet e paligjshme.

Shqetësimet për pastrimin e parave nëpërmjet monedhave virtuale burojnë nga fakti se shumica e emrave të përdoruesve të monedhave virtuale janë pseudonime dhe se është teknikisht e ndërlikuar të identifikohen përdoruesit pas një transaksioni.[4]

Karakteristika të tjera që favorizojnë përdorimin e monedhave virtuale për pastrimin e produkteve të veprës penale janë aksesi dhe shtrirja globale. Në metodat tradicionale të pagesave, kufijtë kombëtarë kufizojnë shumë kohën e përpunimit dhe transferimit të monedhës fizike. Në të kundërt, monedhat virtuale janë monedha globale dhe u mundësojnë kriminelëve të lëvizin shpejt fondet përtej kufijve kombëtarë.[5]

Për më tepër, transfertat e parave nëpërmjet kripto-monedhave paraqesin një realitet financiar mjaft joshës për organizatat dhe elementët terroristë për të legjitimuar burimin e të ardhurave si dhe për të bërë pagesa kundrejt subjekteve apo entiteve të paautorizuara falë anonimitetit të transfertave. Anonimiteti në bërjen dhe marrjen e pagesave, shpejtësia e lëvizjes së parave, thjeshtësia e ruatjes *online* të kripto-monedhave, dhe mungesa e kufizimeve

3 Crowther, P., Hatfield, L., Herbet, J. *European Regulatory Reactions to the Rise of Cryptocurrencies.* Tetor 2019: https://www.winston.com/en/thought-leadership/european-regulatory-reactions-to-the-rise-of-cryptocurrencies.html [Aksesuar 20.05.2022]

4 Schaaf, M. *Is the FATF travel rule effective in the fight against money laundering via virtual currencies.* 2021. Faqe 31. https://theblockchaintest.com/uploads/resources/Uni%20of%20Amsterdam%20-%20Is%20the%20FATF%20travel%20rule%20effective%20in%20the%20fiht%20against%20money%20laundering%20via%20virtual%20currencies%20by%20Marte%20Schaaf%20-%202021%20-%20Jan.pdf [Aksesuar 02.06.2022]

5 Po aty.

gjeografike të transfertave janë karakteristika të kripto-monedhave që i bëjnë ato ndër modalitetet e preferuara të pastrimit dhe transferimit të parave mes subjekteve terroriste.[6]

Qarkullimi i të ardhurave në formën e kripto-monedhave gjithashtu favorizon kushtet për evazion fiskal duke qenë se palët e përfshira në një transaksion financiar mbeten anonime.

Së fundmi, kripto-transaksionet ekspozojnë një sërë rreziqesh për konsumatorët në mjedisin virtual të tilla si: mashtrimi, praktikat tregtare spekulative, dhe pirateria informatike.

Një sërë incidentesh hakërimi kanë përfshirë vjedhjen e njësive paguese virtuale dhe në shkëmbimet e kriptoaseteve. Të gjitha këto rreziqe lidhen me faktin se blerësi nuk ka garancitë e mjaftueshme për të verifikuar autenticitetin dhe rrjedhimisht, legjitmitetin e palës me të cilën përfshihet në një transaksion financiar. Një ndër incidentet më të bujshme të hakërimit të kriptomonedhave përfshin vjedhjen e mbi 400 milionë dollarëve njësi NEM nga shkëmbimi japonez Coincheck. Hakerët vodhën fondet nga portofoli online i *Coincheck*-ut.[7]

2. Gjurmueshmëria e transfertave të kripto-aseteve

Sipas rregullave të reja, të gjitha transfertat e kripto-aseteve duhet të përmbajnë informacion mbi burimin e asetit dhe përfituesin e tij, informacion i cili duhet t'i bëhet i ditur autoriteteve përgjegjëse shtetërore. Rregullat e reja zbatohen gjithashtu mbi të ashtuquajturat "portofolet e paadresuara" (një adresë portofoli e cila nuk është në ruajtjen e një përdoruesi privat).

Direktiva e 2018-ës kërkon që Shtetet Anëtare të BE-së të sigurojnë që regjistrat kombëtarë të pronësisë të personave juridikë përfitues të krijuara nga Direktiva e 2015-ës kundër pastrimit të parave[8] të jenë të aksesueshme për publikun. Subjekteve të detyruara u kërkohet të japin informacion "adekuat, të saktë dhe të përditësuar" për pronarët e tyre përfitues për të

6 Sadon, T. 5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies. 2021. https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies[Aksesuar 06.20.2022]

7 Elliptic. *Financial Crime Typologies in Cryptoassets*. Shtator 2020, faqe 38. https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf [Aksesuar 06.20.2022]

8 Neni 3 paragrafi 6 (a) (i) i Direktivës (BE) 2015/849 për parandalimin e përdorimit të sistemit financiar për qëllime të pastrimit të parave ose financimit të terrorizmit, përcakton si pronarë përfitues personat fizikë që zotërojnë ose kontrollojnë më shumë se 25% plus një aksion ose më shumë se 25% të pronësisë së personit juridik.

siguruar saktësinë e regjistrave të pronësisë së përfituesve.

Subjektet e detyruara duhet të sigurojnë publicitetin, cilësinë e të dhënave dhe aksesueshmërinë e informacionit të pronësisë përfituese të të gjithë subjekteve të tyre juridike, brenda regjistrave kombëtarë të pronësisë përfituese, në përputhje me legjislacionin kombëtar.[9]

3. Bashkëpunimi dhe shkëmbimi i informacionit midis subjekteve rregullatore

Direktiva 2018/483/BE forcon gjithashtu bashkëpunimin dhe shkëmbimin e informacionit ndërmjet mbikëqyrësve financiarë. Direktiva kërkon që shtetet anëtare të BE-së të krijojnë regjistra të centralizuar të llogarive bankare ose sisteme të rikuperimit, për identifikimin e mbajtësve të llogarive bankare dhe llogarive të pagesave. Regjistra dhe sisteme të tilla do të jenë në dispozicion të Njësive të Inteligjencës Financiare ("FIU") të shteteve anëtare të BE-së, për të lehtësuar bashkëpunimin më të mirë me njëri-tjetrin, si dhe me autoritetet e tjera përgjegjëse.

Direktiva vendos mbi shtetet anëtare detyrimin për të krijuar regjistra kombëtarë të centralizuar me mekanizma të automatizuar dhe sisteme elektronike të marrjes së të dhënave për të mundësuar identifikimin e personave fizikë ose juridikë dhe kontrollin e pagesave dhe llogarive bankare. Në këtë drejtim, Shtetet anëtare caktojnë si administratorë të regjistrit qendror të bankës, bankën e tyre qëndrore kombëtare. Ky regjistër qendror duhet të jetë i aksesueshëm për njësitë e inteligjencës financiare dhe autoritetet e tjera.

4. Forcimi i rregullave mbi transaksionet më vendet me risk të lartë

Direktiva 2018/843/BE paraqet një regjim të përmirësuar të ushtrimit të kujdesit të duhur lidhur me transaksionet me vende të treta të identifikuara nga Komisioni Evropian si vende me rrezik të lartë për shkak të mangësive në kuadrin e luftës kundër pastrimit të parave.

Për çdo transaksion me klientët që ndodhen në këto vende, kërkohet informacion shtesë për klientin si: identifikimi i pronarit përfitues, përcaktimi i marrëdhënies së biznesit, mbledhja e informacionit mbi qëllimin

9 Paragrafi 16 i Direktivës 2018/843/BE.

e transaksioneve të synuara ose të kryera, marrja e miratimit të strukturave të larta menaxhuese lidhur me krijimin ose vazhdimin e marrëdhënies së biznesit, si dhe monitorimi i zgjeruar i marrëdhënieve të biznesit duke rritur numrin dhe kohën e kontrolleve, dhe duke zgjedhur modelet e transaksioneve që kanë nevojë për shqyrtim të mëtejshëm.[10] Lista e miraturar nga Komisioni Evropian përfshin në total 23 shtete.[11]

Në zbatimin e masave monitoruese ndaj subjekteve që operojnë në vendet me risk të lartë, shtetet anëtare duhet të marrin në konsideratë sipas rastit, vlerësimet ose raportet e hartuara nga organizatat ndërkombëtare dhe autrotitetet e tjera kompetente në fushën e parandalimit të pastrimit të parave dhe luftës kundër financimit të terrorizmit lidhur me rreziqet që paraqesin vende të treta individuale.[12]

5. Zgjerimi i numrit të subjekteve të detyruara

Direktiva 2018/843/BE zgjeron fushën e zbatimit të direktivave të mëparshme të BE-së në luftën kundër pastrimit të parave, duke zgjeruar listën e subjekteve që detyrohen të regjistrojnë transaksionet financiare.

Së pari, në dallim nga Direktiva e 2015-ës, Direktiva 2018/843/BE vendos në radhët e subjekteve të detyruara jo vetëm audituesit, llogaritarët e pavaruar, dhe këshilluesit e taksave, por dhe çdo person tjetër që merr përsipër të ofrojë, drejtpërdrejt ose me anë të personave të tjerë me të cilët ai person tjetër është i lidhur, ndihmë materiale, ndihmë ose këshilla për çështje tatimore si veprimtari kryesore e biznesit ose profesionale.[13]

Së dyti, listës së subjekteve të detyruara i shtohen një numër subjektesh të reja të cilët janë[14]: ofruesit e shërbimeve të ruajtjes së portofolit (virtual); ofruesit e shërbimeve të këmbimit të monedhave virtuale me para fizike; tregëtuesit në fushën e arteve kur shuma e transaksionit është më e lartë ose e barabartë me 10, 000 (dhjetëmijë) euro; dhe agjentët e pasurive të patundshme që veprojnë si ndërmjetës në dhënien me qira të pronës kur qiraja mujore i kalon 10,000 (dhjetëmijë) euro.

Gjithashtu, shtetet anëtare duhet të ndalojnë institucionet e tyre të kreditit

10 Neni 1 paragrafi 11 i Direktivës 2018/843/BE.

11 Shih: European Commission adopts new list of third countries with weak anti-money laundering and terrorist financing regimes. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_781 [Aksesuar 06.16.2022]

12 Neni 1 paragrafi 11 i Direktivës 2018/843/BE.

13 Neni 1 paragrafi 1, pika (a) i Direktivës 2018/843/BE.

14 Po aty, pika (b) dhe (c).

dhe institucionet financiare që të mbajnë llogari anonime, libreza anonime ose kasaforta anonime. Shtetet anëtare, në çdo rast, duhet të ndërtonin mekanizma të cilat siguronin që pronarët dhe përfituesit e llogarive ekzistuese anonime, librezave anonime ose kasafortave anonime t'u nënshtroheshin masave të kujdesit të duhur ndaj klientit jo më vonë se data 10 janar 2019.[15]

6. Ulja e shumës limit të transaksioneve financiare me karta të parapaguara

Direktiva 2018/843 ul pragun sipas të cilit ofruesit e shërbimeve financiare kanë detyrimin të identifikojnë transaksionet në para elektronike me karta të parapaguara. Përdorimi anonim i kartave të parapaguara do të lejohet vetëm në dy rrethana, e konkretisht: (1) për klientët që bëjnë blerje në dyqan nën 150 euro, duke ulur pragun e mëparshëm prej 250 euro; dhe (2) kur një klient kryen një transaksion në internet me një kartë me parapagesë nën 50 euro.[16]

Vendeve anëtare të BE-së u kërkohet gjithashtu të sigurojnë që kartat anonime të parapaguara të lëshuara jashtë Bashkimit Evropian të mos përdoren në territorin evropian, përveç rasteve kur ato plotësojnë kërkesat e përmendura më sipër.

7. Kufizimet në fushën e veprimit të Direktivës 2018/843/BE

Regjimi i vendosur nga Dirketiva 2018/843/BE shënon një hap të rëndësishëm përpara në forcimin e besueshmërisë së insitucioneve financiare dhe parandalimin e përdorimit të sistemit financiar për pastrimin e produkteve të veprës penale, duke ulur anonimitetin në transaksionet e kripto-aseteve, rritur transparencën mbi natyrën dhe burimin e tyre, si dhe duke forcuar bashkëpunimin dhe shkëmbimin e informacionit midis sektorit financiar dhe strukturave të përfshira në luftën kundër parandalimit të pastrimit të parave.

Megjithatë, mes studiuesve dhe operatorëve të fushave përkatës ekziston mendimi se fusha e veprimit të Direktivës mbetet e kufizuar për aq sa i takon natyrës së transaksioneve të mbuluara prej rregullimit të saj.

Mendimi dominues është që Direktiva 2018/843 nuk adreson transfertat person-me-person të realizuara pa përdorimin e shërbimeve ndërmjetëse të

15 Neni 1 paragrafi 6 i Direktivës 2018/843/BE.

16 Neni 1, paragrafi 7 i Direktivës 2018/843/BE.

tilla si platformat e tregtimit të bitkoin-ave. Këto transaksione mbeten jashtë rregullimit duke qenë se kemi të bëjmë me operacione të shkëmbimit të monedhave virtuale mes tyre dhe jo të monedhave virtuale me para fizike.

Direktiva 2018/843 nuk adreson faktin që monedhat virtuale, krahas shkëmbimit me para letre, përdoren edhe për një sërë qëllimesh të tjera si blerja e shërbimeve ose e mallrave, shkëmbimi me lloje të tjera të monedhave virtuale të përdorimi në transaksione kripto-kripto, pa kërkuar angazhimin apo ndërmjetësimin e ofruesve të propozuar si "subjekte të detyruara". Kjo është në kontrast me praktikën e SHBA-së, ku rregulloret aktuale mbulojnë edhe transaksionet kripto-me-kripto.[17]

Një qëndrim kritik mbi regjimin rregullues aktual lidhet gjithashtu me faktin se përshirja në radhët e subjekteve të detyruara të ofruesve të shërbimeve të ruajtjes së portofolit virtual nuk zgjidh plotësisht anonimitetin që karakterizon transaksionet e kripto-aseteve. Monedhat virtuale mund të transferohen midis individëve (të ashtuquajturët portofolet e pastrehuar) pa përdorimin e një ndërmjetësi.

Subjektete kriminale mund të përdorin portofolet virtuale të pastrehuara (të paregjistruara në emër të një ndërmjetësi) për t'iu shmangur rregullave të regjistrimit dhe raportimit. Prandaj, një pjesë e transaksioneve të monedhës virtuale do të mbeten të pamonitoruara dhe në një mjedis anonim.[18]

Një tjetër problematikë që ngrihet nga studiuesit është mungesa e qartësisë në pëkufizmin e termit "monedhë virtuale". Direktiva në dispozitën për monedhat virtuale nuk trajton me mjaftueshmëri natyrën e avancuar teknologjike të monedhave virtuale. Sipas përkufizimit në fjalë, është e paqartë nëse rregullat e saj gjejnë zbatim ndaj shërbimeve të grumbullimit dhe rishpërndarjes së monedhave virtuale të projektuara posaçërisht për të siguruar anonimitet të plotë të zotëruesit, të njohura këto si shërbimet "tumbler" ose "mixer". [19]

Po ashtu, nuk është e qartë nëse përkufizimi aktual i monedhës virtuale është projektuar për të përfshirë aktivitetet e lojërave të fatit *online*. Nëse

17 Apostolopoulou, I. *A proposal for EU regulation on Bitcoin*. 2018. Faqe 52. http://arno.uvt.nl/show.cgi?fid=146844 [Aksesuar 07.07.2022]

18 European Parliament. Provisional Agreement Resulting from Interinstitutional Negotiations. Dhjetor 2017. http://www.europarl.europa.eu/RegData/commissions/econ/inag/2017/1220/CJ12_AG(2017)616577_EN.pdf [Aksesuar 07.07.2022]

19 Shih më sipër: Apostolopoulou, I. *A*Faqe 52. Për më shume mbi natyrën e shërbimeve "tumbler" dhe
"mixer" shih: Stevens, B. *Bitcoin Mixers: How Do They Work and Why Are They Used? 2022.* https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used [Aksesuar 01.09.2022]

regjimi i Direktivës 2018/843 nuk targeton këto shërbime, një pjesë e madhe e transaksioneve të kripto-monedhave do të mbeten anonime.

Së fundmi, nuk është e qartë nëse Direktiva gjen zbatim ndaj njësive dixhitale të paprekshme të njohura ndryshe si NFT. Njësitë NFT shërbejnë për të përcaktuar të drejtat e pronësisë mbi asetet dixhitale. Ato ofrojnë një mjet për të përfaqësuar zotërimin ose pronësinë e aseteve dixhitale si lojërat, arti dhe muzika.[20]

Direktiva 2018/843 nuk ofron një përkufizim të qartë të "veprave të artit" dhe nuk përcakton ose përmend specifikisht njësitë dixhitale të paprekshme. Për rrjedhojë, nuk është e sigurt nëse NFT-të do të konsiderohen si vepra arti sipas Direktivës dhe si të tilla, t'i nënshtrohen rregullave të Direktivës në luftën kundër pastrimit të parave.

Direktiva nuk ofron detaje të qarta mbi kërkesat e raportimit për NFT-të, pavarësisht shtrirjes së saj rregullatore në shkëmbimet e monedhës virtuale dhe shërbimet e ruajtjes së portofolit virtual. Një shpjegim i mundshëm është se, në vitin 2018 kur u miratua direktiva, NFT-të nuk njiheshin dhe përdoreshin gjerësisht, dhe si rrjedhim, qëndruan jashtë fushëveprimit rregullator të regjimit ligjor të BE-së për luftën kundër pastrimit të parave.[21]

Boshllëku rregullator mbi njësitë e paprekshme të të drejtave të pronësisë dixhitale (NFT) mund të rrisë rrezikun e transaksioneve me vlerë të lartë me të tilla njësi, me qëllim përdorimin e tyre si një mjet për të anashkaluar rregullat kundër pastrimit të parave në nivel të BE-së. NFT-të mund të tregtohen lehtësisht pasi ato nuk kanë një përfaqësim fizik ose mjet transportues, duke siguruar një nivel të lartë anonimiteti në transaksionet e tyre. Për më tepër, ato janë të lidhura me kripto-monedhat të cilat po përdoren gjithnjë e më shumë në skemat e krimit të rëndë dhe të organizuar, si dhe të mashtrimit në investime.

Në përfundim, mund të themi që patjetër legjislacioni i BE-së ka ndryshuar në vazhdimësi për të mbyllur për aq sa është e mundur çdo shteg që mund të shfrytëzohet për pastrimin e parave, apo financimin e terrorizmit, veçanërisht kur bëhet fjalë për përdorimin e portofoleve anonime të kripto-monedha. Megjithatë, në realitetin e sotëm kur teknologjia ecën me ritme shumë të shpejta, dhe kjo teknologji përdoret edhe për qëllime të paligjshme, vendet anëtare dhe vetë Bashkimi Europian i kushtojnë në vazhdimësi vëmendjen e duhur përmirësimit të legjislacionit në këtë drejtim.

20 Kafteranis, D., Abukari, A., Turksen, U. *Money Laundering Via Non-Fungible Tokens.* https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/05/money-laundering-non-fungible-tokens

21 Po aty.

Bibliografia

Apostolopoulou, I. *A proposal for EU regulation on Bitcoin*. 2018. http://arno.uvt.nl/show.cgi?fid=146844

Crowther, P., Hatfield, L., Herbet, J. *European Regulatory Reactions to the Rise of Cryptocurrencies.* Tetor 2019. https://www.winston.com/en/thought-leadership/european-regulatory-reactions-to-the-rise-of-cryptocurrencies.html

Direktiva 2018/843/BE *"Mbi ndryshimin e Direktivës (BE) 2015/849 për parandalimin e përdorimit të sistemit financiar për qëllimet e pastrimit të parave ose financimit të terrorizmit, dhe ndryshimin e Direktivave 2009/138/KE dhe 2013/36/BE"*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

Elliptic. *Financial Crime Typologies in Cryptoassets*. Shtator 2020. https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf

European Parliament. *Provisional Agreement Resulting from Interinstitutional Negotiations.* Dhjetor 2017, http://www.europarl.europa.eu/RegData/commissions/econ/inag/2017/1220/CJ12_AG(2017)616577_EN.pdf

Kafteranis, D., Abukari, A., Turksen, U. *Money Laundering Via Non-Fungible Tokens.* https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/05/money-laundering-non-fungible-tokens

Sadon, T. 5 *Reasons Why Criminals & Terrorists Turn to Cryptocurrencies*. 2021. https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies

Schaaf, M. *Is the FATF travel rule effective in the fight against money laundering via virtual currencies.* 2021. https://theblockchaintest.com/uploads/resources/Uni%20of%20Amsterdam%20-%20Is%20the%20FATF%20travel%20rule%20effective%20in%20the%20fiht%20against%20money%20laundering%20via%20virtual%20currencies%20by%20Marte%20Schaaf%20-%202021%20-%20Jan.pdf

Stevens, B. *Bitcoin Mixers: How Do They Work and Why Are They Used? 2022.* https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/

CIP Katalogimi në botim BK Tiranë
Grup autorësh
The role of technology in preventing and combating organized crime, finacial and corruption : international academic conference : book of proceedings / Grup autorësh. - Tiranë : Graphic Line-01, 2023. - 944 f. : 16.5 x 24.5 cm.
ISBN 9789928470737
1.Krime të organizuar 2.Teknologjia e informacionit 3.Konferenca
343.9 (062)
004 (062)