CZU 343.98:007 DOI: https://doi.org/10.5281/zenodo.20827896

THE APPLICABILITY OF ARTICLE 8 OF THE ECHR TO THE OFFENCE OF COMPUTER FRAUD: LIMITS OF DIGITAL INVESTIGATIONS AND REQUIREMENTS OF A FAIR TRIAL

Daniel CREȚU MARIO,
Specialist Officer,
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
ORCID: 0009-0008-9591-2796

Sergiu CERNOMOREȚ,
PhD, Associate Professor,
"Ștefan cel Mare" Academy of the Ministry of Internal Affairs,
Associate Professor, "Lower Danube" University of Galați,
ORCID: 0000-0003-0172-0491

Abstract

This article examines the relevance of the European Court of Human Rights' case-law to the investigation and punishment of computer-related fraud, with particular emphasis on the Convention limits applicable to digital surveillance and electronic evidence.

The paper starts from the premise that, although the Court does not adjudicate cybercrime offences as such and does not create an autonomous criminal policy model in this field, its case-law substantially shapes the European legal framework through the standards developed under Articles 8, 6 and 7 of the European Convention on Human Rights. From that perspective, the study argues that the Court's relevance in the field of computer-related fraud lies primarily in controlling the proportionality of state interference, protecting digital privacy, safeguarding adversarial proceedings and equality of arms in relation to digital evidence, and preserving the requirements of legal certainty and foreseeability in criminal law.

Keywords: computer-related fraud, cybercrime, digital evidence, privacy, fair trial, Budapest Convention, international cooperation.

INCIDENȚA ART. 8 DIN ChEDO CU PRIVIRE LA INFRACȚIUNEA DE FRAUDĂ INFORMATICĂ: LIMITELE INVESTIGAȚIEI DIGITALE ȘI EXIGENȚELE UNUI PROCES ECHITABIL

Abstract

Prezentul studiu analizează relevanța jurisprudenței Curții Europene a Drepturilor Omului pentru investigarea și sancționarea fraudei informatice, din perspectiva limitelor convenționale impuse utilizării tehnologiilor de supraveghere și administrării probelor digitale.

Lucrarea pornește de la premisa că, deși Curtea nu judecă direct infracțiuni informatice și nu configurează un model autonom de politică penală în materie, jurisprudența sa influențează decisiv cadrul juridic european prin standardele dezvoltate în aplicarea articolelor 8, 6 și 7 din Convenție. Din această perspectivă, cercetarea urmărește să evidențieze că relevanța CEDO în domeniul fraudei informatice constă mai ales în controlul proporționalității ingerințelor statului, în protecția vieții private digitale, în exigențele contradictorialității și egalității armelor în raport cu probele electronice, precum și în menținerea cerințelor de claritate și previzibilitate ale normei penale.

Cuvinte-cheie: fraudă informatică criminalitate informatică, probe digitale, viață private, proces echitabil, Convenția de la Budapesta, cooperare internațională.

Introduction. The rapid expansion of digital technologies has profoundly changed not only the way economic and social activities are carried out, but also the forms in which criminality manifests itself. In this new context, computer fraud has emerged as one of the most dynamic and difficult-to-control forms of crime, as it exploits both the technical vulnerabilities of information systems and the legal difficulties generated by the cross-border nature of the digital environment [1, pp. 1-2]. It is no longer merely a technological adaptation of classical fraud, but rather a type of unlawful conduct that simultaneously raises issues of jurisdiction, evidence, international cooperation and the protection of fundamental rights [34, pp. 148-149].

From a legal perspective, combating computer fraud cannot be reduced to the mere expansion of the state's repressive powers. On the contrary, the effectiveness of digital investigations depends on the ability of authorities to act within a normative framework that allows access to electronic evidence, the monitoring of certain communications or the use of computer data, without turning these instruments into a space of arbitrariness [4, pp. 25-26]. It is precisely at this point that the case-law of the European Court of Human Rights becomes relevant. Although the Court does not adjudicate cybercrime offences as such, it establishes the conventional standards against which the means used by states in investigating and sanctioning such acts must be assessed [28, pp. 2-3].

This the study aims to determine the extent to which ECtHR case-law influences the manner in which European states may investigate computer fraud without exceeding the limits imposed by the Convention. The hypothesis of the paper is that the relevance of the ECtHR in this field does not lie in the direct regulation of cybercrime, but in the configuration of a set of legal requirements concerning the protection of private life, the legality of interferences, the administration of digital evidence and the guarantees of a fair trial [27, p. 8]. In other words, the Court does not provide a criminal-law model of computer fraud, but rather a model for controlling state power in the context of digital investigations.

The analysis of the relevant case-law of the European Court of Human Rights, combined with the examination of the main European and international instruments in the field of cybercrime, forms the basis of the present research [28, p. 144].

From a methodological perspective, the study combines normative analysis with case-law analysis, while also taking into account a critical doctrinal perspective. Its objective is not to provide an exhaustive inventory of the forms of computer fraud, but to highlight the legal standards that condition the legitimacy of the state's response to this phenomenon.

Discussions and results obtained. I. Computer Fraud between Technological Specificity and Legal Vulnerability. Computer fraud differs from traditional forms of fraud through the nature of the environment in which it is committed, the instruments used and the particular manner in which the harmful result is produced. In the digital environment, obtaining an unlawful patrimonial advantage does not always require direct contact with the victim or the physical presence of the perpetrator in a specific place. Instead, it may result from the manipulation of information systems, deception through electronic means, the compromise of authentication data or the fraudulent use of payment and communication infrastructures [2, p. 79].

This form of criminality has a strongly adaptive character. Methods of operation evolve alongside technology, and the speed with which new digital tools emerge often makes the normative response of states slower than the dynamics of the acts under investigation [32, p. 127]. From this perspective, the fundamental challenge is not merely the

criminalisation of conduct, but the maintenance of a functional correspondence between the legal norm, technological reality and the requirements of the protection of fundamental rights.

Moreover, computer fraud almost always has a transnational dimension. The perpetrator may act from one jurisdiction, the technical infrastructure may be located in another, while the victims and evidence may be dispersed across several states. Such a structure complicates the determination of jurisdiction, access to data, cooperation between authorities and the use of electronic evidence [34, p. 144]. Consequently, the legal response to computer fraud cannot be conceived exclusively in terms of domestic criminal law, but requires an articulation between criminal law, criminal procedure, judicial cooperation and the European protection of human rights.

At the same time, the phenomenon produces a major economic and social impact. Patrimonial damage, the erosion of trust in digital infrastructures and the increase of risks to the security of electronic transactions transform computer fraud into a problem that goes beyond the strictly criminal sphere [31, p. 4]. For this reason, its prevention and repression require an integrated approach, in which repressive instruments are complemented by technical measures, international cooperation and digital education [41]. However, legitimate this objective may be, it cannot automatically justify the unlimited expansion of surveillance or data collection. In a state governed by the rule of law, the effectiveness of combating cybercrime must be assessed in relation to the conventional limits of state intervention [8].

In order to provide continuous education, training and information in the field of cybercrime, it is necessary to: develop and implement training programs dedicated to employees with investigative and criminal prosecution duties, prosecutors, judges and technical personnel [35, p. 510].

II. The European Legal Framework: Between Normative Harmonisation and Conventional Control. At European level, the fight against cybercrime is carried out through a multi-layered legal architecture. At its foundation lies the Budapest Convention on Cybercrime, which represented the first international instrument with a comprehensive scope in this field, by establishing common standards concerning both the criminalisation of offences and international cooperation, as well as the procedural powers necessary for their investigation [4]. The importance of the Convention lies not only in its harmonising function, but also in the fact that it expressly reflects the need to strike a balance between law-enforcement interests and respect for fundamental rights.

European Union law complements this framework through legal instruments concerning the security of networks and information systems, data protection, access to electronic evidence, and operational cooperation between Member States. Naturally, these instruments do not replace domestic law, but they create pressure towards normative and institutional convergence, especially with regard to responses to new forms of digital crime [6]. On the other hand, normative harmonisation does not eliminate the risk of imbalances between the repressive logic of criminal law enforcement and the requirements of human rights protection, thus highlighting the distinct role of the European Court of Human Rights.

The Court does not define cybercrimes and does not establish the constituent elements of computer fraud; its function is entirely different: to review whether, in the process of preventing, investigating and sanctioning such offences, states comply with the guarantees of the Convention [28, p. 3].

From this perspective, the case-law of the European Court of Human Rights be-

comes relevant not because it constructs a criminal law of cybercrime, but because it establishes the legality parameters of the state's response. The interception of communications, the monitoring of internet use, access to digital data, the storage of information concerning online activity, the use of technical surveillance measures and the use of electronic evidence all fall within an area in which Article 8 and Article 6 of the Convention acquire decisive importance [13]. In certain situations, Article 7 also becomes relevant, especially where technological developments risk creating tension with the requirements of clarity and foreseeability of criminal law provisions [25].

Therefore, the European legal framework in the field of computer fraud cannot be understood merely by listing the applicable legal instruments. It must also be analysed from the perspective of the conventional control exercised by the Court, which requires states to demonstrate that the effectiveness of digital investigations is not achieved through the unjustified sacrifice of individual freedoms [10].

III. CEDO Case-Law and the Standards Applicable to Digital Investigations. 3.1. Protection of Private Life and the Limits of Electronic Monitoring. A first perspective relevant to the investigation of computer fraud concerns the protection of private life and correspondence in the digital environment. In Copland v. the United Kingdom, the Court held that the monitoring of a person's electronic communications, including e-mail and internet use, falls within the scope of protection of Article 8 of the Convention. The importance of this judgment does not lie in its direct connection with computer fraud, but in the clarification of an essential principle: information generated through the use of communication technologies is not excluded from conventional protection merely because it is produced in a professional or digital environment [13].

This approach is particularly important in the field of investigations concerning computer fraud, since the gathering of evidence often involves access to communications data, online activity history or the content of electronic exchanges. In such situations, the Court requires that the interference be prescribed by law, pursue a legitimate aim and be necessary in a democratic society [26]. It follows that the technical effectiveness of monitoring is not sufficient; it must be accompanied and reinforced by a clear normative framework and by safeguards against arbitrariness.

The same logic can also be found in Bărbulescu v. Romania, in which the Court emphasised the obligation of national authorities to ensure a fair balance between the employer's legitimate interest and the employee's right to private life and correspondence. Although the case belongs to the field of labour law, its value goes beyond the strict framework of professional relationships. It highlights that the mere technical possibility of monitoring does not, in itself, justify the legitimacy of such interference. For the field of computer fraud, this conclusion is important because it shows that the monitoring of communications and digital behaviour must be subject to a rigorous proportionality review [7].

Consequently, the Court's case-law suggests that the protection of private life in the digital environment does not operate as an absolute obstacle to criminal investigations, but as a criterion for disciplining them. The state may use technical monitoring tools, but only insofar as the legal basis, the aim pursued and the procedural safeguards prevent the investigation from turning into excessive surveillance [10].

3.2. Legality and the Use of Digital Evidence. A second central and relevant idea concerns the legality of evidence and the relationship between irregularities in obtaining it and the requirements of a fair trial. In *Khan v. the United Kingdom*, the Court held that Article 6 does not, as a general rule, establish an autonomous system for the admissibility

of evidence, since this matter falls primarily within the scope of domestic law. The decisive issue is whether the proceedings, assessed as a whole, were fair [15].

This approach has important consequences for the use of digital evidence in computer fraud cases. In practice, electronic data may be obtained through methods that raise issues of legality, authenticity or reliability. However, an irregularity in the method by which evidence was obtained does not automatically lead to the conclusion that Article 6 has been violated. Rather, the Court examines whether the accused party was able to challenge the evidence, whether the court critically assessed its credibility and whether the proceedings as a whole provided sufficient safeguards [15].

In *Bykov v. Russia*, the Court emphasised the need for adequate safeguards against abuses in the use of covert methods of obtaining evidence [9]. The relevance of this case-law to the digital environment is clear. In the current context, technical instruments for data collection, recording, digital infiltration or access to information systems allows authorities a high degree of intrusion. In the absence of clear limits and effective control, such instruments may become incompatible with the requirements of the Convention [10].

Therefore, the issue of digital evidence is not limited to the question of whether such evidence is useful or effective. It also requires an assessment of the legality of the manner in which it was obtained, the conditions under which it may be challenged and the institutional safeguards accompanying its use in criminal proceedings.

3.3. The Right to a Fair Trial and the Adversarial Principle in the Digital Era. The right to a fair trial acquires a particular significance in the field of cybercrime, since digital evidence may be technical, opaque and difficult for the accused person to understand. In *Schenk v. Switzerland*, the Court held that the use of unlawfully obtained evidence does not automatically amount to a violation of Article 6, provided that the proceedings, viewed as a whole, remain fair [20]. This idea has been consistently reiterated in subsequent case-law and constitutes an important point of reference in the assessment of electronic evidence [15].

In relation to such evidence, the requirements of Article 6 imply more than the mere formal presence of the evidence in the case file. The accused person must have an effective opportunity to know, understand and challenge the digital material used against him or her. The adversarial principle and equality of arms become essential where the evidence is highly technical, produced by complex information systems or derived from technical operations that the party cannot easily verify [11].

This means that, in matters concerning computer fraud, the fairness of the proceedings depends not only on the formal legality of data collection, but also on the conditions under which such data are introduced, explained and challenged before the Court. The more technical and less immediately accessible the digital evidence is, the more important the role of the court becomes in ensuring the effective exercise of the rights of the defence [14].

3.4. Article 7 and the Requirement of Foreseeability of Criminal Law. Although studies on computer fraud usually focus on Article 8 and Article 6, Article 7 of the Convention is also relevant. The principle of legality of offences and penalties requires criminal law provisions to be sufficiently clear and foreseeable so as to enable individuals to understand the legal consequences of their conduct [17]. In the field of cybercrime, this requirement may become problematic precisely because of the accelerated pace of technological change [32, p. 4].

Computer fraud is an area in which new patterns of conduct often emerge before

legal terminology and legislative techniques have had time to adapt. In such a context, the temptation to use excessively broad formulations may increase. However, such an approach risks weakening the foreseeability of the law and undermining legal certainty. The relevance of Article 7 lies precisely in recalling that the modernisation of criminal law cannot be achieved by sacrificing the requirement of clarity [17].

From this perspective, the contribution of the European Court of Human Rights is indirect but essential: it warns that the need for legislative adaptation to new technological realities does not exempt the state from the obligation to formulate criminal law provisions compatible with the requirements of legality [27].

3.5. The Real Relevance of ECtHR Case-Law for Combating Computer Fraud. The Court's case-law does not provide an autonomous model of criminal policy in the field of computer fraud. It does not determine which investigative techniques are the most effective, nor does it define operational strategies for combating digital crime. Its relevance is, however, fundamental at another level: that of the legitimate limitation of state power and of conditioning the use of technological instruments on compliance with conventional guarantees [28].

In this respect, the impact of the European Convention on Human Rights on the fight against computer fraud is structural. The Court requires states to construct their investigative practices in a manner compatible with private life, the legality of interferences, adversarial proceedings, the rights of the defence and the foreseeability of the legal norm. This influence is all the more important as digital investigations tend to expand the state's capacity to collect, correlate and use large volumes of information [27].

Therefore, the Court's real contribution does not consist in reducing the effectiveness of the fight against cybercrime, but in preventing it from shifting towards a security model devoid of safeguards. In a democratic society, the effectiveness of repression cannot be achieved by suspending rights, but only by integrating them into the very logic of the criminal-law response [16].

IV. Current Problems and Challenges in Combating Computer Fraud. The fight against computer fraud currently faces a permanent tension between the rapid pace of technological transformation and the relative inertia of legal mechanisms. Offenders use encryption, anonymised infrastructures, advanced social engineering and, increasingly, tools based on artificial intelligence, which complicates the identification of perpetrators, the location of evidence and the documentation of offences [29, pp. 12-13]. Consequently, law-enforcement authorities are placed in a position where technical superiority no longer belongs exclusively to public authority.

Another major difficulty concerns access to electronic evidence. Relevant data may be dispersed across borders, held by private providers, encrypted or stored for limited periods of time. In this context, delays in international cooperation may decisively affect the effectiveness of the investigation [34, p. 47]. However, the operational pressure generated by these difficulties may encourage insufficiently regulated intrusive measures, which is why conventional control remains indispensable [10].

The problem of normative fragmentation also persists. Although harmonisation instruments exist, differences between national legislations, procedural standards and institutional practices continue to create a space of legal vulnerability that can be exploited by criminal networks [40, p. 147]. For this reason, international cooperation should not be understood merely as an instrument of assistance between authorities, but as a structural element of the effective fight against computer fraud [3, Art. 23].

The preventive dimension must not be ignored either. Insufficient digital literacy,

users' vulnerability to online manipulation techniques and excessive trust in platforms and electronic means facilitate the expansion of computer fraud [21, pp. 4-5]. In the absence of a minimum culture of digital security, criminal repression inevitably remains belated.

Under these circumstances, an effective legal response cannot be exclusively punitive. An integrated approach is necessary, combining legislative adaptation, the strengthening of international cooperation, the development of technical investigative capacities and the digital education of users. Only such a combination can realistically reduce the gap between the mobility of cybercrime and the state's capacity to respond within the limits of the rule of law [41].

Conclusions. The analysis carried out in this study highlights that computer fraud represents one of the most complex manifestations of contemporary crime, both through the technological specificity of its methods of commission and through the legal and procedural difficulties it generates. The adaptable nature of this phenomenon, its frequently transnational dimension and the central role of digital evidence mean that the state's response cannot be conceived exclusively in terms of classical criminal repression. Combating computer fraud necessarily requires a constant adjustment of the relationship between the effectiveness of investigations and respect for fundamental rights.

The study has shown that the relevance of the case-law of the European Court of Human Rights in this field does not lie in the direct regulation of computer fraud, but in the establishment of legal standards applicable to state intervention in the digital environment. From this perspective, the Court functions as an essential benchmark for assessing the legitimacy of surveillance measures, the use of electronic evidence and the manner in which authorities exercise their powers during criminal investigations. Its contribution is therefore one of delimitation and control, as it imposes clear limits regarding interferences with private life, the requirements of procedural fairness and the demands of legality.

An important finding of the research is that the protection of private life remains a central element even in the context of intensified digital investigative measures. The monitoring of communications, access to data and the use of modern technical means are not, in themselves, incompatible with the need to combat computer fraud, but they become legitimate only insofar as they are clearly regulated, proportionate to the aim pursued and subject to effective safeguards against arbitrariness. At the same time, the use of digital evidence requires increased attention from the perspective of the right to a fair trial, since its technical complexity may genuinely affect the accused person's ability to know, understand and challenge it.

The study also highlights that the rapid evolution of technology does not diminish the importance of the principle of legality, but rather reinforces its relevance. The adaptation of legislation to new forms of cybercrime is necessary, yet it cannot take place at the expense of the clarity and foreseeability of criminal law provisions. In the absence of sufficiently precise criminal offences and coherent procedural rules, the legal response risks becoming unstable and vulnerable from the perspective of fundamental rights protection.

At the same time, the transnational dimension of computer fraud confirms that the effectiveness of its prevention and repression depends essentially on international cooperation. However, the need for speed and efficiency in exchanging data and obtaining evidence cannot justify the circumvention of legal safeguards. On the contrary, it is precisely in the context of cross-border cooperation that maintaining a balance between the repressive interest and the protection of individual freedoms becomes essential.

Ultimately, computer fraud requires a model of legal response based on the complementarity between effectiveness and safeguards. The case-law of the European Court of Human Rights provides the necessary benchmarks for constructing this balance, demonstrating that the protection of fundamental rights is not an obstacle to combating cybercrime, but a condition of its legitimacy. Only through the coherent integration of these standards into legislation, judicial practice and the activity of criminal investigation authorities can an effective, proportionate response compatible with the requirements of the rule of law be built.

Bibliographical references

1. Clough Jonathan. A *World of Difference*: *The Budapest Convention on Cybercrime and the Challenges of Harmonisation*. In: Monash University Law Review, Vol. 40, No.3, 2014, pp.1-2; 20.
2. Clough Jonathan. Principles of Cybercrime. Cambridge University Press, 2nd ed., 2015, pp.7-10; 78-80.
3. Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, Preambul; Art. 1, Art. 2-8, Art. 23-35.
4. Council of Europe, Explanatory Report to the Convention on Cybercrime. Budapest, 23.11.2001, pct. 16-20; 22-23; 33-39; 44-50; 71-80; 145-148; 243-256.
5. Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime, 2021, pct. 7-10, pp. 2-3.
6. Directive (EU) 2022/2555 — NIS2 Directive, OJ L 333, 27.12.2022, pp. 80-152.
7. ECtHR [GC], Bărbulescu v. Romania, No.61496/08, 5 September 2017, §§ 70-73; 120-122; 133-134.
8. ECtHR [GC], Big Brother Watch and Others v. the United Kingdom, Nos.58170/13, 62322/14 and 24960/15, of 25.05.2021, §§ 322-330; 332-347; 350; 425.
9. ECtHR [GC], Bykov v. Russia, no. 4378/02, 10 March 2009, §§ 78–83; 89–90.
10. ECtHR [GC], Roman Zakharov v. Russia, No.47143/06, of 04.12.2015, §§ 227-234.
11. ECtHR [GC], Rowe and Davis v. the United Kingdom, No.28901/95, of 16.02.2000, § 60.
12. ECtHR, Cantoni v. France, No.17862/91, of 15.11.1996, § 29.
13. ECtHR, Copland v. the United Kingdom, No.62617/00, of 03.03.2007, §§ 41-44.
14. ECtHR, Doorson v. the Netherlands, No.20524/92, 26 March 1996, § 72.
15. ECtHR, Khan v. the United Kingdom, No.35394/97, 12 May 2000, §§ 34-37.
16. ECtHR, Klass and Others v. Germany, No.5029/71, 6 September 1978, §§ 48-50.
17. ECtHR, Kokkinakis v. Greece, No.14307/88, 25 May 1993, § 52.
18. ECtHR, Mirilashvili v. Russia, No.6293/04, 11 December 2008, §§ 200-208.
19. ECtHR, S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008, § 101.
20. ECtHR, Schenk v. Switzerland, No.10862/84, 12 July 1988, § 46.
21. ENISA, Awareness and Cyber Hygiene, European Union Agency for Cybersecurity, Online source, n.p.
22. ENISA, ENISA Threat Landscape 2024, European Union Agency for Cybersecurity, 2024, pp.7-8; 15-16; 18-19.
23. EuroMed Justice, Digital Evidence Manual, 2019, pp.15-16.
24. European Court of Human Rights Knowledge Sharing, Guide on Article 7 of the Convention – No Punishment without Law, 2023/2024, pp.6-8.
25. European Court of Human Rights Knowledge Sharing, Note on Unlawfully Obtained Evidence, 2023/2024, pp.1-2.

26. European Court of Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 6; Art. 7; Art. 8; Art. 8 § 2; Art. 46.
27. European Court of Human Rights, Guide on Article 8 of the Convention – Right to respect for private and family life, home and correspondence, 2021/2023, pp.8-10.
28. European Court of Human Rights, The ECHR in 50 Questions, 2024, p.7.
29. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, 2024, pp.12-13; 22-23.
30. Europol, Online Fraud Schemes: A Web of Deceit, Publications Office of the European Union, 2023, pp.4-5.
31. FBI Internet Crime Complaint Center, 2025 IC3 Annual Report, 2026, pp.3-4.
32. Gercke Marco. Understanding Cybercrime: Phenomena, Challenges and Legal Response, International Telecommunication Union, Geneva, 2012, pp.73-75; 123-127; 126-127.
33. INTERPOL, Africa Cyberthreat Assessment Report 2025, 2025, p. 9.
34. Kleijssen Jan, Pierluigi Perri. *Cybercrime, Evidence and Territoriality: Issues and Options*. In: Netherlands Yearbook of International Law 2016, vol. 47, 2017, pp.144-149.
35. Nastas A., Chernomoreț S. *Criminology: Treatise*. Bucharest: Pro Universitaria, 2023, ISBN 978-606-26-1562-8, 686 p.
36. Regulation (EU) 2016/679 — General Data Protection Regulation, OJ L 119, 4.5.2016, pp.1-88.
37. Regulation (EU) 2016/794 on Europol, OJ L 135, 24.5.2016, pp.53-114.
38. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for Electronic Evidence, OJ L 191, of 28.07.2023, pp.118-180.
39. Stoykova Rositsa. *The Right to a Fair Trial as a Conceptual Framework for Digital Evidence*. In: Computer Law & Security Review, 2023, pp.4-7.
40. UNODC, Cybercrime Module 1 – Key Issues: Cybercrime Trends, Section: "Legal Challenges", Online source.
41. UNODC, Cybercrime, Section: "UNODC response".