Acta Universitatis Danubius
JURIDICA

Crimes Against the Safety and Integrity of Computer Systems and Data

Ștefan Tiberiu Ciurea[1]

Abstract: This article explores the issue of computer crimes, analyzing how Romanian legislation addresses these offenses in its New Criminal Code. Additionally, it examines the challenges faced by judicial practitioners in resolving IT-related cases. The rapid evolution of cybercrime requires continuous legislative adaptation to effectively combat it. However, Romania has so far primarily reorganized previous legal texts rather than introducing substantial changes. As a result, judicial authorities are able to keep pace with cybercriminals but have yet to achieve the ability to stay ahead of them.

Keywords: computer crimes; judicial practice; cybercrime; international cooperation; illegal access

1. Introduction

The development of the Internet has profoundly transformed the way we live, providing a platform for a wide range of activities. Unfortunately, this evolution has also led to an increase in illegal activities, with computers serving as tools for both progress and crime (Vasiu, 2001, pp. 5-19).

Due to its transnational nature, cybercrime represents an increasing threat to individuals, states, and the international community. Consequently, efforts to combat

[1] PhD in progress, Doctoral School of Social and Human Sciences, "Dunărea de Jos" University of Galați, Romania, Address: 47 Domnească St., Galați, Romania, Corresponding author tiberiu.ciurea90@gmail.com.

this phenomenon must be intensified on a global scale, both through the establishment of specific regulations and the enhancement of efficient international cooperation (Activity Report of the Romanian Intelligence Service, 2014). The growing danger posed by transborder criminal activities and the urgent need for a more effective and structured approach to their prevention and suppression have led to the adoption of regional and global instruments designed to unify states' efforts in curbing the proliferation of transnational crime (Boroi & Rusu, 2008, p. 2).

The primary motivation of cybercriminals is substantial financial gain with minimal effort, as offenders operate from a simple computer, often located far from their victims. Credit/debit card fraud constitutes a rapidly growing global issue, resulting in massive financial losses worldwide. At the same time, these financial losses serve as capital for organized crime groups, with illicit income being reinvested into the development of other forms of criminal activity.

Preventing and counteracting threats to national security require coordinated efforts, where competent authorities collaborate with specialized services and regional and international partner structures. Over the past decades, the evolution of cooperation among state authorities has demonstrated a positive trajectory, manifesting in various forms, from intelligence and expertise exchanges to participation in specialized events and even joint operations with international partners (European Council, 2024). Nevertheless, although judicial authorities have managed to keep pace with the evolution of cybercrime, they have yet to achieve the capability of staying one step ahead of cybercriminals.

2. Offenses Against the Security and Integrity of Information Systems and Data, as Stipulated in the New Criminal Code

At the national level, certain cyber offenses are currently regulated by the New Criminal Code, Special Part, Title VII – Offenses Against Public Safety, Chapter VI – Offenses Against the Security and Integrity of Information Systems and Data. There are six such offenses, and they fall under the jurisdiction of the Directorate for Investigating Organized Crime and Terrorism (D.I.I.C.O.T.), pursuant to article 11, paragraph (1), point 1, letter a) and point 2 of Government Emergency Ordinance No. 78/2016. These offenses are investigated by officers and judicial police agents from specialized structures within the Romanian Police responsible for combating organized crime, based on delegation orders issued by prosecutors.

2.1. Illegal Access to an Information System, an Offense Stipulated and Sanctioned Under Article 360 of the Criminal Code

The first of these offenses, the crime of illegal access to an information system, constitutes an exception to the general rule, as it falls under the jurisdiction of the Prosecutor's Offices attached to the Tribunals rather than the Directorate for Investigating Organized Crime and Terrorism (D.I.I.C.O.T.), unlike other cyber offenses. In principle, system access refers to any operation through which a functional interaction with the information system is achieved (Bodoroncea & Cioclei, 2014, p. 778). The aforementioned offense is regulated and sanctioned under Article 360 of the Criminal Code and is classified as an endangerment offense, as the occurrence of a specific result is not a requisite element of its legal definition. The incrimination was originally incorporated from article 42 of Law No. 161/2003 on certain measures to ensure transparency in the exercise of public office and dignities, public functions, and in the business environment, as well as on the prevention and sanctioning of corruption. However, this provision was repealed upon the entry into force of the New Criminal Code. Nonetheless, previous legal practice and jurisprudence remain relevant, as the new regulation does not introduce substantive modifications to the content of the offense.

Illegal access to an information system is also classified as a means offense, as it is frequently encountered in cases of concurrent offenses, with the primary purpose of accessing an information system being the commission of another criminal act. For this reason, in numerous instances documented in judicial case law, the offense under discussion is found in concurrence with another offense, either from the category of crimes against the security and integrity of information systems and data or from those against property. For example, in cases involving the illegal transfer of funds from a bank account, perpetrators often employ phishing techniques to obtain the victim's data. This involves sending an email containing a fraudulent link, purportedly from the victim's bank, under the pretext of requiring personal data updates. Upon accessing the link, victims enter their login credentials into deceptive fields specifically designed by the perpetrators. At this point, the offenders gain access to the victim's online or mobile banking credentials (username and password), seize control of their bank funds, and execute unauthorized transfers. These funds are typically directed either to third-party accounts—whose holders are themselves fraud victims—or, more recently, to electronic wallets containing cryptocurrency. In the aforementioned scenario, judicial practice generally qualifies the legal classification of the act as illegal access to an information system, in ideal

concurrence with the offense of fraudulent financial transactions, which is regulated and sanctioned under article 250 of the Criminal Code (a property-related offense).

Regarding the legal classification commonly applied in judicial practice, courts tend to retain the aggravated form of the offense of illegal access to an information system (paragraphs 2 and 3) even in cases where the means of access involves the use of real credentials that have been obtained or used in an unlawful manner. For instance, this applies when a husband accesses his wife's personal mobile device using her password, which he knows but is not legally entitled to use. The rationale behind the aggravated form is also applicable in such situations, given that the only legal requirement is that the access be "restricted". The incriminating provision does not impose any specific condition regarding the precise manner in which the restriction is violated (Bodoroncea & Cioclei, 2014, p. 779).

Compared to Law No. 161/2003, the previous incriminating provision, the New Criminal Code differs only in terms of the penal sanctioning regime, as defendants now benefit from a more favorable law due to the revised sentencing limits, which range from 2 to 7 years of imprisonment.

Therefore, the primary objective associated with the types of illicit activities in which this offense is encountered consists essentially in harming the patrimony of either natural or legal persons. Judicial practice has demonstrated that, due to the manner in which the incriminating provision is formulated, this offense is capable of covering most emerging scenarios encountered in case law, making it highly relevant and effective in contemporary legal practice.

2.2. Illegal Interception of a Transmission of Computer Data, an Offense Stipulated and Sanctioned Under Article 361 of the Criminal Code

The offense of illegal interception of a transmission of computer data, as regulated and sanctioned under article 361 of the Criminal Code, consists of "the unlawful interception of a non-public transmission of computer data that is intended for an information system, originates from such a system, or is carried out within an information system" (Parliament of Romania, 2009, art. 361). Previously, this offense was regulated under article 43 of Law No. 161/2003, which addressed measures to ensure transparency in the exercise of public offices and dignities, public functions, and the business environment, as well as the prevention and sanctioning of corruption, maintaining the same legal content. The concept of interception, in this context, refers to the capture or acquisition of a data transmission or an

electromagnetic transmission. Consequently, this offense can only be committed through the use of specific technical means designed for such activities (Bodoroncea & Cioclei, 2014, p. 781).

The offense is classified as an endangerment offense, being consummated at the moment of capturing the transmission or emission, regardless of how the perpetrator subsequently interacts with the computer data thus obtained. Attempt to commit this offense is punishable under the provisions of article 366 of the Criminal Code. This offense is regarded as a complementary incrimination in relation to the offense of illegal access to an information system, as the two are frequently found in a consequential connection. As a result, judicial practice has encountered difficulties in technically distinguishing the material acts that fall within the scope of this offense from those specific to illegal access to an information system. Consequently, the offense of illegal interception of a transmission of computer data has been retained only in isolated cases and factual situations, with relatively few instances in practice. Furthermore, a theoretical and practical debate exists regarding the legal classification of installing skimming devices on ATM slots. A small number of magistrates associated this modus operandi with the offense of illegal interception of a transmission of computer data. However, this interpretation was not upheld by the High Court of Cassation and Justice in Decision No. 15 of 14.10.2013, which was issued to resolve a legal unification appeal concerning this matter (Trancă & Trancă, 2014, pp. 50-51).

From a penal sanctioning perspective, article 361 of the Criminal Code constitutes a more favorable criminal law compared to article 43 of Law No. 161/2003, given its sentencing limits of 1 to 5 years of imprisonment.

2.3. Alteration of the Integrity of Computer Data, an Offense Stipulated and Sanctioned Under Article 362 of the Criminal Code

Article 362 of the Criminal Code provides for and sanctions the third cybercrime under this chapter, namely the alteration of the integrity of computer data, which consists of "the modification, deletion, or deterioration of computer data, or the restriction of access to such data, without right" (Parliament of Romania, 2009, art. 362). This offense was previously incriminated under article 44(1) of Law No. 161/2003, maintaining the same legal content, but this provision was repealed with the entry into force of the New Criminal Code. The offense has an alternative content, meaning that the commission of multiple material acts corresponding to

different modalities constitutes a single offense, provided they affect data processed within the same information system**.** Additionally, the alteration of the integrity of computer data is classified as a result-based offense, being consummated at the moment when the integrity or availability of the data is compromised. Pursuant to article 366 of the Criminal Code, attempt to commit this offense is punishable (Dobrinoiu et al., 2014, p. 839).

According to judicial case law developed thus far, the three aforementioned offenses often exhibit an interdependent existence in numerous situations. For instance, the use of software designed for the fraudulent interception of computer data, such as Trojan-type malware, to capture usernames and passwords for widely used applications like Facebook, Gmail, or Yahoo! Messenger, is frequently followed by the modification of access credentials. This act naturally results in the restriction of access for the legitimate account holder. Thus, while the offense of altering the integrity of computer data may initially appear to be an endangerment offense, it is, in fact, a result-based offense. This classification arises from the requirement that actual harm be inflicted—either upon system owners (in cases involving the modification, deletion, or deterioration of computer data) or upon legitimate system users (when access to computer data is unlawfully restricted) (Dobrinoiu, 2006, pp. 180-183).

Article 362 of the Criminal Code, with its sentencing limits of 1 to 5 years of imprisonment, constitutes a more favorable criminal law compared to article 44(1) of Law No. 161/2003.

2.4. Disruption of the Functioning of Information Systems, an Offense Stipulated and Sanctioned Under Article 363 of the Criminal Code

The offense of disrupting the operation of computer systems, as regulated and sanctioned under article 363 of the Criminal Code, consists of “the act of seriously disrupting, without right, the functioning of a computer system by introducing, transmitting, modifying, deleting, or deteriorating computer data, or by restricting access to such data” (Parliament of Romania, 2009, art. 363). This incrimination reiterates the provisions of article 45 of Law No. 161/2003, which was repealed upon the entry into force of the New Criminal Code**.**

Essentially, this offense has an alternative content, is result-based, and constitutes an endangerment offense, being regulated to protect computer systems from cyberattacks or other malicious activities aimed at rendering such systems

inoperative. The transmission of computer data involves sending, inserting, or remotely copying data into the targeted computer system. In principle, disruption consists of modifying the operational parameters of the attacked system, and its severity must always be assessed in relation to the manner in which the system is used, the purpose it serves, the activities it supports, and the domain to which it is attached (Dobrinoiu et al., 2014, p. 854).

The offense can exist independently in situations that are less frequently encountered in judicial practice and are commonly associated with hacking activities, provided that such activities do not also pursue the objective of obtaining material benefits (Trancă & Trancă, 2014, pp. 53-54).

With sentencing limits ranging from 2 to 7 years of imprisonment**,** article 363 of the Criminal Code constitutes a more favorable legal provision compared to article 45 of Law No. 161/2003.

2.5. Unauthorized Transfer of Computer Data, an Offense Stipulated and Sanctioned Under Article 364 of the Criminal Code

The offense regulated under article 364 of the Criminal Code, designed to protect the confidentiality of computer data, serves as a complementary incrimination to the offenses of illegal access to an information system and illegal interception of a transmission of computer data**.** However, judicial practice has recognized the existence of this offense in only a limited number of cases. Previously, this incrimination was found in article 44(2) and (3) of Law No. 161/2003, a provision that was repealed upon the entry into force of the New Criminal Code. Regarding the constitutive elements of the offense, the regulations in the two legislative acts do not differ, with the current legislation consolidating both the standard and assimilated forms of the offense into a single provision. This offense is result-based, consisting of an infringement upon the confidentiality or availability of computer data when such data is moved. Pursuant to article 366 of the Criminal Code**,** attempt to commit this offense is punishable.

The lack of relevant judicial case law concerning the commission of this offense is primarily due to the technical overlap between the computer means used to commit this act and those employed for illegal access to an information system. A cyber offender, as evidenced by the available probative material, acts with direct yet subtle intent. The profile of the cybercriminal reveals a meticulous and obsessive adversary, fixated on a singular objective: without any authorization or consent for the transfer

of computer data, they migrate data from one information system with a specific hardware or software configuration (e.g., a fixed workstation) to another system with a different configuration (such as a storage device—hard disk, USB stick, CD, or DVD). Both copying data and extracting and relocating data fulfill the constitutive elements of the offense. In the latter case, the data can no longer be found in its original location, thereby infringing upon its availability and confidentiality (Bodoroncea & Cioclei, 2014, p. 785).

Legal doctrine demonstrates that the typicality of the offense is also met when data is printed or transferred onto paper, as this operation involves the transfer of data between the computer system and the printer, whose software converts the data into impulses that ultimately enable the printing process. The incriminating provision establishes as an accessory condition the unauthorized nature of the transfer. This condition is fulfilled in two scenarios: (I) when the perpetrator lacks legitimate access to the data, or (II) when, despite having authorized access, they are not permitted to transfer the data or are only permitted to do so under specific conditions, which they fail to comply with (Dobrinoiu et al., 2014, p. 364).

Article 364 of the Criminal Code, with its sentencing limits ranging from 1 to 5 years of imprisonment, constitutes a more favorable criminal law compared to article 44(1) and (2) of Law No. 161/2003.

2.6. Illegal Operations with Devices or Computer Programs, an Offense Stipulated and Sanctioned Under Article 365 of the Criminal Code.

The offense regulated and sanctioned under article 365 of the Criminal Code, the last offense in Chapter VI of Title VII of the Special Part, concerns illegal operations with devices or computer programs and consists of: “The act of a person who, without authorization, produces, imports, distributes, or makes available in any form: (a) Devices or computer programs designed or adapted for the purpose of committing any of the offenses provided for in articles 360-364; (b) Passwords, access codes, or other similar computer data that allow full or partial access to a computer system, with the intent of committing any of the offenses provided for in articles 360-364. The unauthorized possession of a device, computer program, password, access code, or other computer data as described in paragraph (1), with the intent of committing any of the offenses under articles 360-364, also constitutes an offense.” (Parliament of Romania, 2009, Art. 365). This legal provision reiterates and reformulates the same typical elements as those found in article 46 of Law No. 161/2003, which was

repealed upon the entry into force of the New Criminal Code.

The legal provision is designed to protect the security and integrity of information systems and data, as well as their confidentiality and availability. Furthermore, the legal norm criminalizes the preparatory acts of the offenses stipulated under articles 360-364 of the Criminal Code. In its standard form, as outlined in paragraph (1), the offense has an alternative content, meaning that the commission of material acts described through different normative modalities (such as production or import) constitutes a concurrence of offenses, even when they pertain to the same material object.

The terms production and import require no additional clarification, as they refer to the creation and introduction into the country of the goods specified in the legal provision. However, it should be noted that import is difficult to conceive in relation to passwords or access codes, as these are more appropriately covered by the other modalities. The distribution of computer-related materials implies their dissemination to one or more recipients. Making them available refers to facilitating access for other individuals to devices, programs, or computer data in the perpetrator's possession. The possession of such goods constitutes a mitigated form of the offense, as each of the previously mentioned modalities inherently involves possession. For this reason, given that they share the same material object, the offense is classified as one with alternative content (Bodoroncea & Cioclei, 2014, pp. 786-787).

The computer programs referenced by the legislator include, for instance, programs designed to alter or destroy computer data or to interfere with the operations of information systems. These also encompass programs specifically created or adapted to enable and control access to computer systems, such as Trojans or other types of malicious software contaminants (Vasiu, 2016, p. 889).

The offense of illegal operations with devices or computer programs constitutes an abstract endangerment offense, meaning that its consummation does not require the production of a specific result, nor does it depend on whether any of the offenses stipulated under Articles 360-364 of the Criminal Code have actually been committed. The offense is deemed consummated at the moment of the production, sale, import, distribution, making available, or possession—without authorization—of a device, computer program, password, access code, or computer data, provided that such acts are carried out with the intent to commit any of the aforementioned offenses (Amza & Amza, 2003, pp. 28-29).

According to Criminal Sentence No. 163/06.05.2016 of the Cluj Tribunal, the installation of keylogging software on an individual's laptop for the purpose of unauthorized data transfer meets the constitutive elements of the offense of illegal operations with devices or computer programs, as stipulated under article 365(2) of the Criminal Code.

Article 365 of the Criminal Code, with its sentencing range of 6 months to 3 years, constitutes a more lenient criminal law in comparison to article 46 of Law No. 161/2003.

The attempt to commit the offenses discussed in this chapter aligns with the provisions of the previous legislation and was also punishable under the former legal framework, in accordance with article 47 of Law No. 161/2003.

3. Modes of Operation and Cyber Threats

As a rule, cybercrime targets computers, networks, or other forms of information and communication technology. It encompasses, for instance, the creation and dissemination of malware, phishing schemes aimed at stealing banking data, and denial-of-access attacks designed to inflict financial harm and reputational damage.

Cyberattacks with the most significant negative impact are generally those driven by financial motives, such as ransomware, banking trojans, and phishing. However, any type of cyber threat represents an increasingly prevalent reality, affecting entities ranging from high-level state institutions to ordinary users of information systems.

Citizens are exposed to cyber risks through two distinct mechanisms: direct targeting and the compromise of state institutions, which indirectly impacts the population. The assessment of cyber threats is a complex process, driven by attackers' ability to develop sophisticated methods for evading security systems and executing highly precise targeted attacks.

A safe, open, and secure cyberspace appears increasingly difficult to achieve, as preventing such attacks is practically impossible. For instance, the simplest and most well-known form of phishing involves creating a fraudulent link that mimics the interface of online commercial platforms. Essentially, a phishing attack victim posts a sales advertisement for their own item on websites[1], and within minutes, they are contacted via the messaging service by a purported buyer who claims to be interested

[1] Such as www.olx.ro.

in purchasing the product without requesting any additional details. During the conversation, the perpetrator proposes the so-called "OLX shipping method" to the victim, claiming that it involves the buyer making a bank transfer payment before receiving the product, allowing the seller to access the funds immediately. Through this unusually attractive proposal, the perpetrator successfully diverts the victim's attention and sends a fraudulent link[1]. Upon accessing the link, the victim is instructed to enter their bank card number, expiration date, CVV security code, and account balance—despite the fact that receiving a payment would typically require only the account holder's name and IBAN code. Furthermore, victims receive a text message from their bank on their personal phone number containing a 3D Secure code meant to authorize a payment in various currencies (e.g., Ukrainian hryvnias, Russian rubles). However, under the false impression that they are receiving money, victims enter this code into the fraudulent link, unknowingly confirming a transaction instead of receiving funds in their account.

The possibilities for creating such fraudulent links are virtually limitless, requiring only a few seconds to generate. These links are never identical, and they become inactive immediately after the fraudulent transaction is completed, making such offenses nearly impossible to prevent and, in many cases, difficult to combat. By its very nature, cybercrime transcends borders and evolves rapidly—often at a pace faster than national authorities can respond. Victims file criminal complaints, claiming they have been defrauded; however, by that point, it is already too late. Once the fraudulent link becomes inactive, it can no longer be accessed, rendering the identification of the perpetrator's location or the operational domain of the fraudulent webpage virtually impossible.

Ransomware is characterized by the encryption of an entity's data by cybercriminals, who subsequently demand a financial ransom for decryption and the restoration of access. According to data from the European Union Agency for Cybercrime, the average ransom payment has experienced an exponential increase in recent years, doubling in value (European Union Agency for Cybersecurity, 2020).

Malicious software, commonly referred to as malware, is designed to compromise the integrity, availability, or confidentiality of an information system. Its defining characteristics include the ability to propagate covertly within the target system, evade detection mechanisms, neutralize security software, self-update, and download additional malicious components. The primary objective of malware is the

[1] Such as https://www.olx-ro-save.ru.

unauthorized exfiltration of sensitive information, such as authentication credentials, financial data, and other confidential records.

Email-based attacks are attempts to steal access passwords or payment credentials associated with credit cards through various techniques, such as phishing and spam. Cyber fraud schemes related to COVID-19 have been predominant within email threat campaigns (European Union Agency for Cybersecurity, 2020).

DDoS (Distributed Denial-of-Service) attacks are cyber assaults that prevent users of a network or system from accessing information, services, and other essential resources by overwhelming targeted websites with massive traffic from multiple sources. The most recent notable DDoS attack recorded in Romania occurred in the context of the war in Ukraine, when several websites belonging to public institutions, political parties, and private organizations in Romania[1] were subjected to such attacks. The attacks were later claimed by the pro-Russian cybercriminal group "Killnet" via a communication channel on the Telegram mobile application. Members of the group justified their actions by stating that the Romanian government supports Ukraine in its military conflict with Russia (National Cyber Security Directorate, 2022).

4. International Cooperation and Technology-Driven Crime

The phenomenon of cyberattacks and cybercrime is intensifying and diversifying at an international level. The European Council emphasizes the persistent nature of this trend, relying on projections that indicate an increase in the number of Internet of Things (IoT) connected devices to 22.3 billion by 2024 (European Council, 2021).

The collection of electronic evidence for cybercrime investigations can be challenging due to the volatility of digital data and always requires specialized expertise. Judicial cooperation is essential to ensure the timely preservation of electronic evidence, guaranteeing its admissibility in legal proceedings. However, international judicial cooperation can be hindered by significant differences in domestic legal procedures (e.g., variations in the criminalization of offenses or regulations on e-evidence retention) and jurisdictional conflicts. The entire phenomenon of cybercrime is reshaping the traditional legal concept of territoriality,

[1] gov.ro, mapn.ro, politiadefrontiera.ro, politiaromana.ro, cfrcalatori.ro, psd.ro, and otpbank.ro.

as the transnational nature of digital evidence is critical to the successful prosecution of cybercriminals.

Operation "The Godfather," supported by Europol, facilitated cooperation among law enforcement agencies from Belgium, Germany, Italy, the Netherlands, Romania, and Sweden, ultimately leading to the dismantling of illegal skimming device factories in Romania and the arrest of members of the criminal organization. The organized crime network was engaged in card cloning and illicit cash withdrawals, causing financial damages amounting to hundreds of thousands of euros. The skimming devices seized during 31 house searches conducted in Bucharest in January 2010 were intended for installation on various types of ATMs used worldwide. Additionally, authorities confiscated hundreds of counterfeit payment cards, raw card data, electronic equipment (including micro cameras and PIN entry devices), as well as tools used for manufacturing counterfeit debit cards. The skimming attacks ceased in the months following the intervention in Bucharest (European Police Office, 2011).

From the perspective of criminal sanctions under Romanian law for cybercriminals, the maximum sentence of three years' imprisonment for most of the offenses previously discussed—often with a real possibility of suspension—is considered excessively lenient in relation to the financial damage inflicted, as these crimes are committed without the use of violence. Most hackers generate substantial financial gains and would readily accept a criminal record in exchange for profits amounting to millions of euros. On the other hand, ideologically motivated cybercriminals, driven by hostility toward the system and capable of compromising national security—at the very least, triggering a state of alert among authorities—would likewise consider such a mild penalty acceptable, given the personal satisfaction derived from the challenge of breaching even the most highly secured information systems.

5. Conclusions

Thus, it can be observed that criminal law tends to perceive cybercriminals as mere "bookish recluses", marginalized by civil society and often regarded as eccentric yet intelligent individuals, ultimately harmless—incapable of using violence or affiliating with organized crime groups. Nothing could be further from the truth. The damage inflicted by these invisible perpetrators, who are not physically present at the crime scene but operate from behind a screen, sometimes thousands of kilometers

away, ranks among the most severe and consequential losses suffered by victims. Whether affecting individuals facing material harm or influential nations enduring reputational damage, the impact of cybercrime is both profound and far-reaching.

Undoubtedly, the rapid evolution of cybercrime will, over time, compel the national legislator to adapt and introduce amendments that extend beyond a mere restructuring of outdated legal provisions. Instead, legislative reforms will aim to enhance the clarity and precision of incriminating texts, addressing controversial legal issues such as the lack of uniform legal classification among law enforcement authorities. Moreover, it can be anticipated that the sanctioning framework will require adjustments and adaptations based on the modus operandi preferred by cybercriminals—methods that are not necessarily those initially foreseen by the legislator. Given the constant advancement of technical tools used by offenders, as well as their ever-evolving ingenuity, legislative responses must remain dynamic and responsive to emerging threats.

In the context of international legal cooperation in criminal matters, states do not maintain a coherent stance regarding the application of criminal law in cyberspace. There is a pressing need to establish an updated international regulatory framework that would facilitate more effective investigation and prosecution of cybercriminals. The principle of dual criminality, which stipulates that an act must be considered a criminal offense in both the requesting and the requested state, remains a governing criterion in transnational criminal investigations. Investigative authorities are unable to conduct inquiries on computer networks located beyond their national jurisdiction.

There is a noticeable lack of cohesion between policymakers and technology experts, as they operate independently and employ distinct professional terminologies. To effectively address the challenges posed by digitalization, close collaboration between these professional groups is imperative in order to develop a unified strategy. Given that most contemporary technology is interconnected within cyberspace, the contribution of cybersecurity experts is essential to this process.

Technological advancements and emerging threats also necessitate that law enforcement authorities gain access to new tools, acquire new competencies, and develop alternative investigative techniques. Authorities must be able to identify, secure, and interpret the data required for criminal investigations and effectively utilize this data as admissible evidence in court proceedings.

Moreover, it would not be incorrect to assert that judicial authorities also require a more in-depth understanding of both theoretical and technical aspects of cybercrime

to prevent potential instances of legal uncertainty or inequity, which might otherwise be erroneously attributed to defective legislation. For judicial practice to achieve beneficial outcomes, it is essential that those responsible for its application possess the necessary expertise—an objective that can only be realized through continuous education, participation in training programs by both law enforcement authorities and the judiciary, and consultation with experts such as representatives of the National Cybersecurity Directorate (formerly CERT-RO) or the Institute for Advanced Technology within the Romanian Intelligence Service. A significant step in this direction has been undertaken by the High Court of Cassation and Justice through its rulings on appeals in the interest of the law or on the clarification of legal matters in criminal cases (Decision No. 15/2013, Decision No. 4/2021, Decision No. 68/2021, etc.), which have enabled judicial bodies to keep pace with the evolving tactics of cybercriminals. However, despite these efforts, they have yet to achieve the capability of staying ahead of such threats.

References

Amza, T. & Amza, C. P. (2003). *Criminalitatea informatică/Cybercrime.* Bucharest: Lumina Lex.

Bodoroncea, G. & Cioclei, V. (2014). *Codul penal. Comentariu pe articole/Criminal Code. Commentary on articles.* Bucharest: C.H. Beck.

Boroi, A. & Rusu, I. (2008). *Cooperarea judiciară internațională în materie penală/International judicial cooperation in criminal matters.* Bucharest: C.H. Beck.

Directoratul Național de Securitate Cibernetică/ National Cyber Security Directorate. (2022, April 29). *DDoS attacks against public and private websites in Romania*. Retrieved from https://dnsc.ro/citeste/press-release-ddos-attacks-agains-public-and-private-websites-in-romania.

Dobrinoiu, M. (2006). *Infracțiuni în domeniul informatic/Computer crimes.* Bucharest: C.H. Beck.

Dobrinoiu, V., Pascu, I., Hotca, M. A., Chis, I., Gorunescu, M., Păun, C., Neagu, N., Dobrinoiu, M., & Sinescu, M. C. (2014). *Noul Cod penal comentat, Partea specială/The New Criminal Code Commented, Special Part.* Bucharest: Universul Juridic.

European Council. (2021). *Infografic – Principalele amenințări cibernetice în UE/Infographic – Main cyber threats in the EU*. European Council, Council of the European Union. Retrieved from https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/.

European Council. (2024). *How the EU combats cyber threats*. European Council, Council of the European Union. Retrieved from https://www.consilium.europa.eu/en/policies/cybersecurity/.

European Police Office. (2011). *Analiza Europol – Raport general privind activităţile Europol/Europol Analysis – General Report on Europol Activities*. Europol. Received from https://www.europol.europa.eu/sites/default/files/documents/ro_europolreview.pdf.

European Union Agency for Cybersecurity (2020). *Raportul ENISA privind situația amenințărilor în anul 2019-2020/ENISA Threat Situation Report 2019-2020.* Retrieved from https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-a-year-in-review-ebook-en-ro.pdf.

Parlamentul României/Parliament of Romania. (2009). *Noul Cod Penal al României (Legea nr. 286/2009), art. 250/New Penal Code of Romania (Law no. 286/2009), art. 250*. Monitorul Oficial, Partea I, nr. 510/Official Gazette, Part I, no. 510.

Trancă, A. & Trancă, D.-C. (2014). *Infracțiunile informatice în Noul Cod Penal/Cybercrimes in the New Criminal Code.* Bucharest: Universul Juridic.

Vasiu, I. (2001). *Criminalitatea informatică/Cybercrime.* Bucharest: Nemira.

Vasiu, I. (2016). *Explicațiile Noului Cod Penal, vol. IV, art. 257-366/Explanations of the New Criminal Code, vol. IV, art. 257-366.* Bucharest: Universul Juridic.