Legal and Administrative Studies, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
No. 1(34), Year XXV, 2026, pp. 221-243

CYBER FRAUD IN THE ERA OF ARTIFICIAL INTELLIGENCE – LEGAL CHALLENGES AND REGULATORY PERSPECTIVES

Mariana-Alina ZISU
ORCID [ID]: https://orcid.org/0000-0003-2778-3749
Email: stefanoaia.mariana@yahoo.com
Affiliation: College of Legal Advisers Suceava,
Federation "Order of Legal Advisers from Romania"

Abstract: *The digital transformation of society and the accelerated development of technologies based on artificial intelligence have significantly changed the way cybercrime manifests itself, leading to the emergence of new forms of cyber fraud, characterized by a high degree of complexity and increased difficulties in the process of identifying and holding perpetrators accountable. The automation of cyber attacks, the use of algorithms capable of generating credible false content, the development of deepfake technologies and the improvement of social engineering methods assisted by artificial intelligence increase the vulnerability of individuals, public institutions and economic operators. In this context, this study analyzes the main legal implications generated by the use of artificial intelligence in the commission of cyber fraud, with a focus on the applicable national, European and international regulatory framework. The research aims to examine the concept of cyber fraud, identify the main ways of using artificial intelligence in criminal activity, as well as evaluate the efficiency of legal mechanisms designed to prevent and combat these acts. The analysis is based on the interpretation of the legislation in force, the use of specialized doctrine and the examination of relevant European and international legal instruments. The study highlights the need for continuous adaptation of legislation and judicial practice to technological evolution, as well as the importance of international cooperation in combating cybercrime. In conclusion, effective protection against cybercrime requires the development of modern legal mechanisms, capable of responding to the challenges generated by the use of artificial*

intelligence, without affecting the fundamental rights and freedoms of the individual.

Keywords: *computer fraud; computer crime; artificial intelligence; criminal law; digital evidence.*

Introduction

The accelerated development of information and communications technology has led to profound transformations in all areas of social, economic and legal life, generating undeniable benefits in terms of streamlining human activities, access to information and the development of the digital economy. At the same time, technological progress has created the premises for the emergence of new forms of crime, characterized by a high degree of complexity, mobility and adaptability. Cybercrime has long exceeded the limits of attacks on computer systems, becoming a transnational phenomenon with major implications for cybersecurity, economic stability and the protection of fundamental rights of individuals (Terec-Vlad, 2025, pp. 78-90).

Within this phenomenon, computer fraud occupies a distinct place due to the diversity of methods of commission and the extent of the damage caused to individuals, public institutions and the business environment. While in the past these crimes involved the use of relatively limited IT techniques, technological evolution has led to the emergence of sophisticated fraud mechanisms based on automation, algorithmic analysis and the exploitation of vulnerabilities in IT systems and human behavior. Currently, cyber attacks are increasingly well-organized, benefit from advanced technological resources and are frequently carried out by criminal groups operating at an international level.

A significant role in this transformation is played by the development of artificial intelligence (Terec-Vlad, and Ungureanu, 2025). Tools based on artificial intelligence can generate audio, video and text content with a high degree of realism, can automate the process of identifying IT vulnerabilities and can facilitate the development of complex phishing, financial fraud or identity theft campaigns. Although these technologies are developed mainly for legitimate purposes and

contribute to economic and social progress, their use for criminal purposes raises particularly complex legal and ethical issues. Thus, artificial intelligence becomes a factor that amplifies the efficiency of traditional methods of computer fraud and contributes to the emergence of new forms of cybercrime.

The complexity of these phenomena is accentuated by the cross-border nature of computer crimes. Perpetrators can act from different jurisdictions, use globally distributed computer infrastructures and exploit differences between national legislative systems. In these conditions, the investigation of computer fraud requires not only the use of modern methods of managing digital evidence, but also effective cooperation between judicial authorities, European bodies and international organizations competent in the field of combating computer crime.

In recent years, the European Union and the Council of Europe have paid particular attention to strengthening the regulatory framework applicable to cybersecurity and the use of artificial intelligence. The adoption of the Regulation on Artificial Intelligence (AI Act), the development of European legislation on the security of networks and information systems, as well as the application of the Budapest Convention on Cybercrime demonstrate the constant concern for adapting legal norms to technological evolution (Corsei, 2025, pp. 88-97). At the same time, in domestic law, the criminalization of computer fraud and the development of the regulatory framework on the management of electronic evidence reflect the need to protect heritage, data and trust in the digital environment.

However, the dynamics of the development of information technologies often exceed the pace at which legislation evolves. The emergence of generative artificial intelligence systems, the development of deepfake technologies, the use of applications capable of reproducing a person's voice or image and the automation of computer attacks generate significant difficulties in the legal qualification of facts, the identification of perpetrators, the management of evidence and the establishment of criminal liability. In this context, an interdisciplinary approach becomes

necessary, combining legal analysis with the understanding of the technical mechanisms used in the commission of crimes.

This study aims to analyze the impact of artificial intelligence on the evolution of computer fraud and to highlight the main legal challenges generated by the use of these technologies in criminal activity. The research aims to examine the regulatory framework applicable in Romanian, European and international law, identify the main forms of manifestation of computer fraud facilitated by artificial intelligence, as well as evaluate the efficiency of existing mechanisms for the prevention, investigation and sanctioning of these crimes. At the same time, the prospects for the development of legislation in the context of technological progress and the need to strengthen international cooperation in the field of combating cybercrime.

In the development of this study, specific methods of legal research were used, namely normative analysis, comparative method, research of specialized doctrine and examination of relevant judicial practice. The interdisciplinary approach adopted aims to highlight the relationship between technological evolution and the adaptation of legal protection mechanisms, starting from the premise that the efficiency of combating computer fraud depends not only on the existence of adequate criminalization norms, but also on the capacity of the authorities to anticipate and manage the risks generated by the use of artificial intelligence in the digital environment.

1. General considerations on computer fraud

1.1. The concept and defining elements of computer fraud

The digital transformation of society has led to significant changes in the way economic, administrative and social activities are carried out, generating unprecedented opportunities for technological development. At the same time, however, digitalization has created the premises for the emergence of new forms of criminal conduct, adapted to the specifics of the computer environment and characterized by the use of digital technologies as an instrument, means or object of illicit activity. In this context, computer fraud represents one of the most dynamic and complex

forms of computer crime, both through the diversity of the ways in which it is committed and through the economic and social impact it produces.

From a legal perspective, computer fraud is characterized by the unauthorized use of computer systems, programs or computer data for the purpose of obtaining an unjust patrimonial benefit or causing damage to another person. The peculiarity of this crime is that the fraudulent mechanism does not always involve direct contact between the perpetrator and the victim, the criminal activity being carried out through information technologies and electronic communications. This characteristic differentiates computer fraud from classic forms of deception and explains the difficulties encountered in identifying the perpetrators and managing evidence.

In Romanian criminal law, the crime of computer fraud is regulated in the Criminal Code, being incriminated as a distinct act from other computer crimes. The legislator aimed to protect the patrimony, trust in computer systems and the security of operations carried out in the digital environment. The material element of the crime may consist, as the case may be, in the introduction, modification, deletion or restriction of access to computer data or in preventing the functioning of an computer system, if these actions are carried out for the purpose of obtaining a material benefit and cause harm to a person (Antoniu (coord.), 2016, pp. 522–534).

Unlike traditional forms of fraud, cyber fraud usually involves the exploitation of technical or human vulnerabilities (Terec-Vlad, and Rusu, 2026, pp. 82-104). In practice, perpetrators use a variety of methods, such as unauthorized access to bank accounts, manipulation of electronic transactions, interception of communications, compromising computer systems, the use of malicious programs or misleading users through social engineering techniques. In recent years, these methods have become considerably more sophisticated by integrating artificial intelligence-based tools, capable of personalizing attacks and reducing the possibility of identifying fraudulent behavior. A defining element of cyber fraud is its transnational nature. The digital infrastructure allows perpetrators to act from any jurisdiction, using servers located in different countries, encryption of communications and automatic anonymization mechanisms.

This reality complicates both the establishment of the competence of judicial authorities and international cooperation in criminal prosecution and enforcement of court decisions (Corsei, Zisu, and Țoncu, 2023, pp. 52-60). For this reason, the effective fight against computer fraud requires the harmonization of national legislation and the development of effective instruments of cooperation between states.

The specialized literature emphasizes that computer fraud can no longer be analyzed exclusively from the perspective of the patrimonial damage caused to the victim. Today, such crimes affect public trust in digital services, the functioning of financial institutions, the security of critical infrastructures and even the stability of economic relations. The size of these effects justifies the approach to computer fraud as a phenomenon of national and European security, which explains the intensification of legislative and institutional efforts to prevent and combat this type of crime (Dobrinoiu, 2020, pp. 640–648).

Currently, the development of artificial intelligence determines a paradigm shift in terms of the way in which computer fraud is committed. Algorithms capable of generating texts, images, audio or video materials with a high degree of realism allow authors to develop methods of deception that are much more convincing than those used in the past. Consequently, the distinction between genuine and fraudulent communication is becoming increasingly difficult, which requires the permanent adaptation of legal and technical mechanisms for preventing, investigating and sanctioning these acts (Dascălu, 2018, pp. 95–118).

Therefore, computer fraud must be understood as a complex crime, in continuous evolution, the dynamics of which are directly influenced by technological progress. The efficiency of combating it depends on the existence of a framework coherent regulatory framework, international cooperation and the capacity of competent authorities to use modern investigative methods, compatible with the specifics of contemporary cybercrime.

1.2. The evolution of cybercrime in the context of digital transformation

Cybercrime has undergone constant evolution, driven by the accelerated pace of development of digital technologies and the expansion of the use of information systems in all sectors of society. While the first cyber incidents were experimental in nature and aimed mainly at demonstrating technical skills or affecting the functioning of information systems, cybercrime is now an organized phenomenon, predominantly oriented towards obtaining significant economic benefits. This transformation reflects the change in the motivation of the perpetrators, but also the adaptation of criminal methods to new technological and economic realities.

The digitalization of financial services, the development of e-commerce, the widespread use of mobile applications and the migration of administrative activities to the online environment have led to an exponential increase in the volume of processed data and the economic value of digital information. In this context, information systems have become attractive targets for criminal groups, which exploit technical vulnerabilities, configuration errors or the lack of an adequate cybersecurity culture. In many situations, the human factor remains the most vulnerable link, with perpetrators resorting to psychological manipulation techniques to gain access to confidential information or financial resources.

A defining characteristic of contemporary cybercrime is the professionalization of criminal activity. In recent years, the emergence of organized structures that operate according to business-specific models has been observed, with roles distributed between developers of malicious programs, administrators of compromised IT infrastructures, financial intermediaries and individuals specialized in the valorization of the proceeds of crime. This organization increases the efficiency of attacks and complicates the work of judicial bodies, since each participant contributes to the achievement of a distinct stage of criminal activity.

Digital transformation has also changed the ways in which computer fraud is carried out. While in the past these involved direct interventions

on IT systems, today perpetrators use complex social engineering techniques, attack automation and tools based on artificial intelligence. Algorithms can analyze large volumes of information available online, identifying the profile of victims and personalizing fraudulent messages so that they appear authentic. This capability significantly increases the success rate of attacks and reduces the possibility of identifying fraudulent behavior by users (Fuerea, 2023, pp. 412–420).

Another relevant phenomenon is the development of clandestine online markets, where personal data, authentication credentials, malicious software and services designed to facilitate cyberattacks are traded. These platforms allow even people without advanced technical knowledge to carry out criminal activities by purchasing already developed tools. Thus, access to sophisticated means of attack is becoming easier, which contributes to the expansion of the criminal phenomenon and the diversification of fraud typologies.

In this context, artificial intelligence produces a significant change in the dynamics of cybercrime. Generative systems can create personalized emails, fake documents, images and extremely convincing audio or video materials, used to mislead victims. Some applications are also capable of automating the identification of IT vulnerabilities and optimizing attack strategies based on previously obtained results. These developments increase the difficulty of preventing and investigating IT fraud and require the development of modern methods of forensic analysis and digital evidence management (Vasiu, and Vasiu, 2021, pp. 57–79).

From the perspective of criminal law, this development generates important challenges regarding the legal classification of the facts, the establishment of criminal participation and the individualization of liability. In situations where artificial intelligence is used exclusively as an instrument of criminal activity, liability lies with the people who design, control or use these systems for illicit purposes. However, the increasing degree of autonomy of some IT applications and the complexity of algorithmic processes require continuous reflection on the adequacy of the existing legislative framework and the need for legal solutions adapted to technological progress.

In conclusion, the evolution of cybercrime demonstrates that technological progress produces ambivalent effects. On the one hand, it contributes to the development of the digital economy and the efficiency of social and economic activities, and on the other hand, it offers new opportunities for criminal activities. In these circumstances, strengthening cybersecurity, improving the regulatory framework and developing international cooperation are essential conditions for limiting the impact of computer fraud and protecting trust in the digital environment.

1.3. Main forms of computer fraud

The diversification of digital services and the expansion of the use of computer technologies have led to the emergence of increasingly varied ways of committing computer fraud. The evolution of these crimes is closely linked to technological development, with perpetrators constantly adapting the methods used to exploit the vulnerabilities of computer systems and user behavior. Currently, computer fraud no longer exclusively targets financial institutions or large companies, but equally affects individuals, public authorities and economic operators of any size.

One of the most widespread forms of computer fraud is phishing, consisting of the transmission of electronic messages that imitate official communications from banking institutions, public authorities or well-known companies, with the aim of obtaining authentication data, banking information or other confidential data. In recent years, traditional phishing methods have been complemented by artificial intelligence-assisted techniques, capable of generating personalized messages, written in natural language and adapted to the profile of each victim. This evolution reduces the possibility of identifying fraud attempts and increases the efficiency of attacks.

Another important category is computer banking fraud, carried out through unauthorized access to bank accounts, manipulation of electronic transactions or fraudulent use of payment instruments. In many situations, the perpetrators combine computer techniques with social engineering methods, causing victims to voluntarily authorize seemingly legitimate

financial operations. The complexity of these frauds is amplified by the use of applications capable of simulating the identity of representatives of financial institutions or reproducing their voices through voice synthesis technologies (Vasiu, and Vasiu, 2022, pp. 123–145).

In recent years, a phenomenon that has been continuously expanding is fraud based on deepfake technology. By using artificial intelligence algorithms, perpetrators can generate images, audio recordings or videos that reproduce with a high degree of fidelity the voice and appearance of a person. These materials are used to mislead victims, obtain financial transfers, compromise the reputation of individuals or facilitate identity theft. The particularity of these frauds lies in the difficulty of verifying the authenticity of digital content and the speed with which false information can be distributed through online platforms (UNODC, 2024, pp. 91–118).

Another frequently encountered modus operandi is the compromise of business electronic communications, known in the specialized literature as Business Email Compromise (BEC). In such situations, perpetrators gain access to the electronic correspondence accounts of a commercial company or create email addresses very similar to the official ones, requesting payments to accounts controlled by criminal groups. The development of artificial intelligence allows the automatic analysis of commercial correspondence and the generation of messages perfectly adapted to the communication style of impersonated persons, which makes the identification of fraud much more difficult.

Fraud involving digital assets and cryptocurrencies is also becoming increasingly common. The popularity of investments in such assets has been exploited by people who create fictitious investment platforms, non-existent projects or pyramid schemes promoted through social networks. Artificial intelligence is used to carry out extremely convincing promotional campaigns, to automatically generate advertising content and to interact with potential victims through conversational applications. These mechanisms increase the credibility of frauds and allow them to expand rapidly internationally.

The use of malicious software designed to obtain financial benefits cannot also be ignored. Ransomware programs, applications that intercept authentication data or tools capable of monitoring user activity are used to

compromise computer systems and obtain significant amounts of money. In many cases, artificial intelligence helps to optimize these programs by automatically identifying vulnerabilities and adapting attack strategies based on the security measures encountered.

The analysis of these forms of fraud highlights the fact that the common element is not exclusively the use of information technology, but the exploitation of user trust and the exploitation of existing technical vulnerabilities. In this sense, artificial intelligence does not create new crimes in the legal sense, but significantly changes the way in which the acts are carried out and the efficiency of the mechanisms used by the perpetrators. This reality requires the continuous adaptation of prevention policies, the development of modern investigative tools and the strengthening of cooperation between national authorities and international bodies competent in combating cybercrime (Europol, 2024, pp. 18–36).

Therefore, the main forms of cyberfraud demonstrate that technological progress is accompanied by legal and social risks that cannot be ignored. Understanding the mechanisms used by perpetrators and the way in which artificial intelligence influences criminal activity is an essential condition for the development of effective legislative and institutional measures, capable of providing an adequate level of protection to individuals, institutions and the business environment.

2. Artificial Intelligence – a factor in the evolution of computer fraud

2.1. The role of artificial intelligence in the commission of computer fraud

Artificial intelligence is one of the most important technological innovations of the 21st century, being used in a growing number of fields, such as medicine, education, industry, public administration, the financial sector and justice. The ability of systems based on artificial intelligence to analyze impressive volumes of data, to identify behavioral patterns and to generate content close to that created by humans has determined a profound transformation of the way in which economic and social

activities are carried out (Russell, and Norvig, 2021, pp. 1–34). At the same time, these characteristics have also been exploited by criminal groups, which use artificial intelligence to develop increasingly sophisticated and difficult to identify fraud methods.

Unlike traditional IT tools, artificial intelligence systems allow the automation of complex processes that previously required the direct intervention of the author. Modern algorithms can quickly analyze the information available in the online environment, identify potential victims and generate messages adapted to their profile. Thus, cyber attacks are no longer carried out randomly, but are personalized according to the behavior, interests or professional activity of the targeted individuals. This personalization considerably increases the efficiency of cyber fraud and reduces the likelihood that victims will identify the attempted deception.

One area in which the influence of artificial intelligence is evident is the automation of phishing campaigns. If in the past fraudulent messages frequently contained errors of expression, general formulations or clues that allowed the identification of their illicit nature, applications based on artificial intelligence currently generate coherent texts, adapted to the context and written in a language close to that used by banking institutions, public authorities or contractual partners. In addition, these systems can instantly translate messages into numerous languages and adapt the content to the cultural peculiarities of the recipients, thus expanding the geographical area of attacks.

Artificial intelligence also contributes to the improvement of social engineering techniques. By analyzing public information available on digital platforms and social networks, algorithms can build detailed profiles of victims, identifying professional relationships, personal preferences and online behavior. This information is then used to develop credible scenarios, in which victims are determined to disclose confidential data, make financial transfers or allow unauthorized access to computer systems. In this way, artificial intelligence transforms social engineering into an automated process, based on the analysis and exploitation of human behavior.

Another relevant aspect is the use of artificial intelligence for the development and optimization of malicious computer programs. Some

applications can automatically identify existing vulnerabilities in computer systems, adapt attack methods depending on detected security measures and modify the structure of the source code to avoid detection by antivirus solutions. This adaptability reduces the effectiveness of classic protection mechanisms and requires the development of security tools based, in turn, on intelligent technologies.

From the perspective of criminal law, the use of artificial intelligence does not change the constitutive elements of the crime of computer fraud, but it influences the concrete way in which the criminal activity is carried out and the complexity of judicial investigations. Criminal prosecution bodies are forced to manage increasingly complex digital evidence, to establish the origin of the algorithms used and to identify the persons who designed, configured or used the computer systems for criminal purposes. In many situations, the difficulties are not generated by the lack of criminalization rules, but by the identification of the perpetrators and the cross-border nature of the criminal activities[1].

In this context, the responsible use of artificial intelligence is becoming a major concern of the European legislator and national authorities. The European Regulation on Artificial Intelligence (AI Act) aims to ensure the development and use of these systems in a manner compatible with fundamental rights, cybersecurity and the principles of the rule of law. While the Regulation does not directly regulate criminal liability for cyber fraud, it establishes obligations on risk management, transparency and control of certain artificial intelligence systems, indirectly contributing to reducing the possibilities of misuse of these technologies (ENISA, 2024, pp. 25–47).

Therefore, artificial intelligence must be seen as a technology with a dual character. Its use contributes to the development of society and to the efficiency of numerous economic and administrative activities, but the same technology can be exploited to commit highly sophisticated

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), Official Journal of the European Union, L 1689/2024.

cybercrimes. This reality requires the continuous adaptation of legislation, the development of modern investigative mechanisms and the strengthening of international cooperation, so that technological progress is accompanied by legal guarantees capable of protecting individuals and institutions against new forms of cybercrime.

2.2. Deepfake, intelligent phishing and digital identity theft

The evolution of generative artificial intelligence has led to the emergence of new ways of committing computer fraud, characterized by a high level of realism and an increased capacity to mislead victims. While traditional fraud methods were mainly based on exploiting technical vulnerabilities of computer systems, new technologies allow the exploitation of human vulnerabilities by creating digital content that is almost impossible to distinguish from authentic content. In this context, deepfake technologies, artificial intelligence-assisted phishing campaigns and digital identity theft represent some of the most serious challenges for judicial bodies and for authorities responsible for cybersecurity.

Deepfake technology uses advanced artificial intelligence models to generate or modify images, audio recordings and video materials, so that they faithfully reproduce the physical appearance, voice and behavior of a real person. Initially developed for legitimate purposes, such as film production, education or research, this technology has also begun to be used for fraudulent purposes. Criminals can create videos or audio recordings in which a person appears to be requesting a bank transfer, the disclosure of confidential information or the approval of a financial transaction. The high degree of authenticity of these materials makes victims place a high level of trust in the content received.

One area in which the use of deepfake technology has particularly serious consequences is represented by financial fraud. Situations have been reported in which employees of companies have authorized transfers of large amounts of money after participating in video conferences or receiving phone calls generated by artificial intelligence, being convinced that they are talking to their hierarchical superiors. Such incidents demonstrate that verifying a person’s identity solely through image or

voice no longer offers the guarantees of authenticity that it offered in the past.

In parallel, phishing has undergone a significant transformation through the use of artificial intelligence. If fraudulent messages could previously be identified by grammatical errors, unnatural expressions or general information, current applications are capable of generating well-structured texts, personalized and adapted to the professional or personal context of each victim. By analyzing the information available on digital platforms and social networks, systems based on artificial intelligence can create messages that reproduce the communication style of a financial institution, a contractual partner or a close person. Under these conditions, the probability that the victim considers the message authentic is considerably higher.

At the same time, artificial intelligence facilitates the development of complex spear phishing attacks, aimed at carefully selected individuals. Unlike classic campaigns, which targeted a large number of recipients, these attacks are built on a detailed analysis of the victim's online activity. Information on the position held, professional relationships, ongoing projects or personal interests is used, which allows the development of credible scenarios that are difficult to identify as fraudulent. In the corporate environment, such attacks can lead to the compromise of internal communications, the disclosure of trade secrets or the production of significant financial damages.

Another consequence of the development of artificial intelligence is the amplification of the phenomenon of digital identity theft. Perpetrators can use images, audio recordings, falsified documents and information obtained from public sources to create credible virtual identities, which are subsequently used in commercial relations or in interaction with financial institutions. In some situations, these identities are used to open bank accounts, contract financial services or carry out other illicit activities, which makes it difficult to identify the perpetrators and recover damages.

From a legal point of view, these developments raise numerous issues regarding the management of evidence and the establishment of criminal liability. Materials generated by artificial intelligence can create

difficulties in verifying the authenticity of digital evidence, and identifying the perpetrator often requires cooperation between authorities from several states and the use of advanced forensic analysis methods. At the same time, the development of these technologies forces the legislator to constantly adapt the rules on data protection, cybersecurity and the investigation of cybercrime.

Faced with these challenges, prevention becomes as important as sanctioning the facts. Public institutions, economic operators and users must adopt additional mechanisms for identity verification, multifactor authentication, internal procedures for confirming financial transactions and permanent training programs on the risks associated with the use of technologies based on artificial intelligence. Equally, the developers of these systems have the responsibility to implement technical measures that reduce the possibility of using applications for fraudulent purposes.

In conclusion, deepfake technologies, smart phishing and digital identity theft demonstrate that artificial intelligence is profoundly changing the nature of computer fraud. These tools increase the ability of perpetrators to manipulate victims and complicate the work of judicial bodies, requiring a continuous adaptation of prevention, investigation and sanctioning mechanisms. In this context, effective protection against computer fraud can no longer be achieved exclusively through technical measures or by criminalizing the acts, but requires an integrated approach, based on institutional cooperation, digital education and the permanent updating of the legislative framework.

2.3. Automation of cyber attacks and vulnerabilities of digital systems

One of the most important consequences of the development of artificial intelligence is the possibility of automating activities specific to cyber attacks. If, in the past, identifying vulnerabilities and carrying out an attack required advanced technical knowledge and considerable preparation time, today many stages of this process can be carried out automatically through applications based on machine learning algorithms. This evolution determines not only the increase in the efficiency of

criminal activities, but also the expansion of access to sophisticated IT tools for people who do not have in-depth technical skills.

Artificial intelligence allows the analysis of a large number of IT systems in a very short time, identifying vulnerable configurations, security errors or outdated applications. Based on this information, algorithms can automatically select the most exposed targets and adapt attack methods depending on the level of protection identified. Thus, the process of preparing a cyber fraud becomes faster, more efficient and more difficult to detect in the early stages.

At the same time, systems based on artificial intelligence can constantly optimize the strategies used by the authors. By analyzing the results of previous attacks, these applications can identify the methods that had the highest success rate and can automatically modify the content of messages, the structure of computer programs or the ways of communicating with victims. This continuous adaptation capacity differentiates modern attacks from classic ones and explains why traditional defense mechanisms become, in some situations, insufficient.

Another phenomenon worth analyzing is the development of the concept of Cybercrime-as-a-Service. This model involves the marketing, through clandestine platforms, of computer services intended for carrying out criminal activities. Malicious programs, compromised computer infrastructures, databases with personal information, communication encryption services or applications that use artificial intelligence to automate attacks can be purchased. Consequently, committing computer fraud is no longer limited to people with advanced technical training, but is becoming accessible to an increasing number of criminals.

Automation also affects the way malware spreads. Some applications can identify vulnerable devices, automatically deliver malicious code, and adapt their behavior to meet security measures. In some cases, AI-based systems are able to evade detection by modifying their own code or by constantly changing the way they communicate with the servers used by the attackers. This flexibility makes it harder for cybersecurity professionals to identify and neutralize threats.

At the same time, the widespread use of cloud computing, internet-connected devices, and complex digital infrastructures is expanding the attack surface. Organizations are managing ever-increasing volumes of information and using interconnected IT systems, meaning that a single vulnerability can impact a significant number of users or services. In this context, protecting digital infrastructure is no longer just a technical issue, but a strategic one, with economic, social, and legal implications.

From a legal perspective, this development requires a reconsideration of the way in which the prevention and investigation of computer fraud are approached. Judicial bodies must have adequate technical resources and specialized personnel to manage digital evidence and to understand the mechanisms used by systems based on artificial intelligence. Equally, cooperation between judicial authorities, institutions responsible for cybersecurity, academia and the private sector is becoming essential for the rapid identification of new criminal typologies and for the development of effective responses.

Particular attention must also be paid to the responsibility of organizations that develop or use complex computer systems. The implementation of effective cybersecurity policies, constant updating of applications, risk assessment and staff training are indispensable measures to reduce the vulnerabilities exploited by criminals. The experience of recent years demonstrates that many computer frauds are not possible solely due to the performance of the technology used by the perpetrators, but also as a result of deficiencies in the organization and management of the system victims' computer themes.

Looking ahead, the development of artificial intelligence will continue to influence both the methods of committing computer fraud and the tools used to combat it. Intelligent algorithms can become an important ally of authorities and cybersecurity specialists by early detection of suspicious activities, analysis of user behavior and automatic identification of fraud attempts. Therefore, the effectiveness of combating computer crime will depend on the ability of society to use the same technological advances to strengthen prevention and protection mechanisms, while maintaining a balance between security, respect for fundamental rights and the development of technological innovation.

3. Legal framework and perspectives on combating computer fraud

Combating computer fraud is one of the most important challenges of contemporary law, given the rapid evolution of digital technologies and the cross-border nature of these crimes. The complexity of the methods used by perpetrators, as well as the integration of artificial intelligence in the process of committing illicit acts, require the existence of a flexible regulatory framework, capable of responding to both current and future technological challenges.

In Romanian law, the protection of social relations regarding the security of computer systems and the patrimony of individuals is ensured by the provisions of the Criminal Code on computer crimes, supplemented by special regulations on the prevention and combating of computer crime and by the rules on cybersecurity. These provisions aim to sanction illegal access to computer systems, the modification or destruction of data, the disruption of the functioning of computer systems and fraud committed through them. However, the application of legal rules faces difficulties generated by the anonymous nature of the digital environment, the use of IT infrastructures distributed in several countries and the accelerated pace of technological development.

At European and international level, the fight against computer fraud is based on cooperation between states and the existence of common legal instruments. The Budapest Convention on Cybercrime is the main international instrument in the field, providing a unified framework for the criminalization of acts, the management of digital evidence and judicial cooperation. At the same time, the European Union has adopted regulatory acts aimed at strengthening cybersecurity and regulating the use of artificial intelligence, aiming to reduce the risks generated by the use of these technologies for illicit purposes.

The adoption of the Regulation on Artificial Intelligence marks an important moment in the development of European law, as it establishes obligations regarding the development, use and supervision of artificial intelligence systems, depending on the level of risk they pose. Although the regulation does not directly regulate criminal liability for cyber fraud,

it helps prevent the misuse of applications capable of generating false content, facilitating user manipulation or automating cyber attacks. At the same time, new European regulations on the security of networks and information systems impose higher standards of protection and responsibility for public authorities and economic operators.

However, the effectiveness of combating cyber fraud does not depend solely on the existence of appropriate legal rules. Investigating these crimes requires the use of modern methods of managing digital evidence, the development of appropriate technical capabilities and increased cooperation between judicial authorities, institutions specialized in cybersecurity and international bodies. The rapid exchange of information, mutual legal assistance and the conduct of joint investigations are indispensable tools in identifying and holding perpetrators accountable, especially when criminal activity is carried out simultaneously in several jurisdictions (Corsei, 2025, pp. 86-98).

From the perspective of technological evolution, it is clear that artificial intelligence will continue to influence both the ways in which cyber fraud is committed and the methods used to prevent and investigate it. In these circumstances, the legislative framework must remain flexible enough to respond to technological changes, without affecting the development of innovation or the exercise of fundamental rights and freedoms. An effective policy in the field of combating cyber fraud involves combining repressive and preventive measures, investing in digital education, strengthening cybersecurity and developing permanent international cooperation. Only through such an integrated approach can the effective protection of individuals, assets and trust in the digital environment be ensured, in a society in which artificial intelligence will play an increasingly important role.

Conclusions

The evolution of digital technologies and the accelerated development of artificial intelligence have led to profound transformations both in society and in the way cybercrime manifests itself. While technological progress offers important opportunities for economic

development, streamlining services and improving the quality of life, it also creates the conditions for the emergence of new forms of cyberfraud, characterized by a high degree of sophistication and an increased capacity to adapt to existing security measures.

The analysis carried out in this study highlights the fact that artificial intelligence is not, in itself, a source of cybercrime, but a technological tool that can be used for both legitimate purposes and criminal activities. The use of intelligent algorithms to automate cyberattacks, generate deepfake content, develop personalized phishing campaigns or facilitate digital identity theft demonstrates that traditional fraud methods have acquired a higher level of complexity, which requires the continuous adaptation of legal and institutional mechanisms for prevention and control.

At the same time, the research reveals that the current national and European legislative framework provides important legal instruments for sanctioning cyber fraud and strengthening cyber security. However, the dynamics of technological development require a permanent update of legal norms, an interpretation adapted to new digital realities and a strengthening of international cooperation in the field of investigating cyber crimes. In this regard, the effective application of the legislation depends not only on the existence of adequate criminalization norms, but also on the capacity of the authorities to use modern investigative means and to capitalize on the technical expertise necessary for the management of digital evidence.

Also, the effective fight against cyber fraud cannot be achieved exclusively through the intervention of criminal law. Reducing the risks generated by the abusive use of artificial intelligence requires the development of a cyber security culture, constant investments in digital education, the implementation of high standards of protection of IT systems and the strengthening of collaboration between public authorities, the private sector, the scientific community and international organizations. Prevention must be as important as punishment, as many cyber frauds primarily exploit human and organizational vulnerabilities.

In the future, the development of artificial intelligence will continue to influence both the ways in which cyber fraud is committed and the tools used to identify and prevent it. For this reason, law must evolve at the same pace as technology, maintaining a balance between stimulating innovation and protecting the fundamental values of society. Only through an integrated approach, based on international cooperation, legislative adaptation, institutional responsibility and the responsible use of emerging technologies, can effective protection against cyber fraud be ensured and citizens' trust in the digital environment be strengthened.

References

Antoniu, G. (coord.) (2016). *Explanations of the new Criminal Code*, vol. IV. Universul Juridic.

Corsei, A. (2025). The impact of artificial intelligence on fundamental human rights. *Journal Legal and Administrative studies (JLAS)*, Volume 33, Issue 2.

Corsei, A. (2025). Artificial Intelligence and the Right to a Fair Trial in the Context of Evidence Administration. *Anuarul Universitatii Petre Andrei din Iasi-Fascicula: Drept, Stiinte Economice, Stiinte Politice [Yearbook of Petre Andrei University of Iasi - Section: Law, Economic Sciences, Political Sciences] Volume* 34.

Corsei, A., Zisu, M.A., and Țoncu, S. (2023). The European Union and fundamental human rights. *AGIR Bulletin*, Issue 4.

Dascălu, I. (2018). *Computer Crime.* Universul Juridic.

Dobrinoiu, V. (2020). *The New Criminal Code Commented. Special Part*, Third Edition. Universul Juridic.

ENISA. (2024). ENISA Threat Landscape 2024. *European Union Agency for Cybersecurity.*

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. *Publications Office of the European Union.*

Fuerea, A. (2023). *European Union Law*, 6th edition. Universul Juridic.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

intelligence (AI Act), Official Journal of the European Union, L 1689/2024.

Russell, S, and Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*, 4th Edition. Pearson.

Terec-Vlad, L. (2025). *Inteligenţa artificială şi securitatea cibernetică în domeniul juridic: provocări, reglementări şi perspective [Artificial intelligence and cybersecurity in the legal field: challenges, regulations and perspectives]*. Universul Juridic, *Volume* 6.

Terec-Vlad, L., and Ungureanu, C.G. (2025). The Rights of Artificial Intelligence: Between Ethics, Law and Normative Pragmatism. *Journal Universul Juridic*.

Terec-Vlad, L., and Rusu, A. (2026). Neuro-Cybersecurity and the Future of Cognitive Rights: Legal Foundations for the Protection of the Human Mind in the Digital Age. *Revista Romaneasca pentru Educatie Multidimensionala*, Volume 18, Issue 1.

UNODC, (2024). Comprehensive Study on Cybercrime. *United Nations Office on Drugs and Crime*.

Vasiu, I., and Vasiu, L. (2021). *Cybercrime*. Universul Juridic.

Vasiu, I., and Vasiu, L. (2022). *Cybercrime and Computer Crime. Comments and Explanations.* Universul Juridic.

.