RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
March 12-13, 2026

DOI:10.5281/zenodo.19553480

Criminal Investigation and the Incidence of AI in the Collection and Management of Digital Evidence

Carmen Silvia Paraschiv

Professor, PhD, Faculty of Law, "Titu Maiorescu" University of Bucharest, Romania
paraschivcrmn@yahoo.com

Abstract: This research paper analyzes the optimization of criminal investigations by integrating artificial intelligence into digital evidence, highlighting the significant impact of emerging technologies on law enforcement processes. In an era characterized by fast digitalization, the contemporary criminal phenomenon has diversified, and the complexity and volume of computer data require an efficient adaptation of investigative tools. This paper analyzes the mechanisms through which artificial intelligence can facilitate the discernment and analysis of digital evidence, thus contributing to the efficiency of criminal investigation activities. Relevant case studies and examples of good practices extracted from different jurisdictions are presented here, highlighting both the functional advantages and the ethical and legal challenges arising from the use of AI technologies in crime-fighting activities. The analysis also includes a discussion of the rigor of evidence standards and procedural guarantees, emphasizing the need for a responsible and transparent application of artificial intelligence in the context of crime investigation. The conclusions suggest that integrating AI into criminal trials can be a viable solution for increasing the efficiency and accuracy of investigations while ensuring compliance with the fundamental principles of law. This paper aims to contribute to the ongoing discourse on technological innovations in criminal law and the reconfiguration of investigative paradigms in line with the demands of a modern society.

Keywords: Artificial Intelligence, Technological Innovations, Criminal Process, Digital Samples Investigations, Efficiency

1. The Judicial System and the Impact of AI on IT

In order to facilitate the process of familiarization with the topic in question, it is appropriate to operate with the famous definition offered by John McCarthy in 1955, from which it is distinguished that artificial intelligence represents the capacity of machines to perform tasks and tasks associated with human intelligence, imitating the way a human function. This includes activities such as natural language processing, image and voice recognition, decision-making and machine learning. Modern artificial intelligence systems are based on machine learning algorithms, which have the ability to learn from data sets and increase their efficiency over time. There is a diversity of types of artificial intelligence, ranging from simple rule-based systems to complex neural networks and advanced deep learning systems. A significant aspect of contemporary artificial intelligence is its ability to process and analyze considerable volumes of data, facilitating the identification of patterns and the formulation of predictions. However, it is essential to note that these systems also have notable limitations, including the dependence on the quality of the data used in the training process and the risk of reproducing biases existing in this information. It is fundamental to realize that artificial intelligence is not a universal solution, and its use must be guided by ethical principles and respect the fundamental rights of the individual (Franguloiu, 2023, p. 40).

The development of artificial intelligence technology presents notable opportunities for the modernization and efficiency of the judicial system. In the context of Romania, where the volume of cases and the complexity of jurisprudence are continuously expanding, the implementation of a specialized artificial intelligence system could represent an innovative solution for improving the quality of the act of justice.

1.1 Intelligent integration of technology in the efficiency of the judicial system: challenges and opportunities

In the context of the modernization and efficiency of the judicial system, the implementation of AI-type Legal solutions proves to be essential for improving the documentation process, the quality of decisions and the optimization of working time. Quick access to relevant case law and the automatic identification of similar judicial precedents, along with an efficient synthesis of legal doctrine, significantly contribute to more efficient documentation. Thus, judges can carry out comprehensive analyses of national and European case law, identifying trends and reducing the risk of inconsistencies in judicial practice. Through the application of advanced machine learning technologies, AI represents a transformative solution with an important role in supporting, accelerating and improving various aspects of investigations in criminal cases, especially complex ones, where AI acts as a "force multiplier" for investigators (Niță et al., 2025, p. 248).

Functionalities such as advanced search engines and recommendation systems promote contextual search and multi-criteria filtering, thus facilitating rigorous documentation. At the same time, drafting assistants offer intelligent templates and useful suggestions, reducing the time spent on repetitive processes. However, implementing these solutions raises technical, ethical and practical challenges, requiring an updated database, integration with existing systems and ensuring data confidentiality. In this regard, the proposed implementation methodology, including the pilot phase and gradual scaling, allows for continuous adjustment of the system based on feedback, thus ensuring an efficient transition to a modernized judicial system adapted to current needs.

1.1.1 AI Regulation in Europe

The development and evolution of regulations on artificial intelligence (AI) is a complex process, influenced by rapid technological advances, concerns about the ethics and security of AI use, and the desire to promote economic innovation. In the 1950s and 1960s, AI was in its infancy, and regulatory concerns were minimal. As technology advanced, questions began to arise about the social and ethical impact of AI. Initial concerns were mainly related to the use of AI in sensitive areas, such as weapons systems or automated decision-making processes. In recent decades, as AI applications have become increasingly ubiquitous, discussions have also emerged about the risks and challenges they pose. These include: discrimination, cybersecurity, and transparency (Brundage et al., 2028).

Over the years, various international initiatives have been developed to address these challenges. For example, the Organisation for Economic Co-operation and Development (OECD, n.d.) has proposed principles for the responsible use of AI, while the United Nations University and other institutions have launched studies and proposals on the regulation of AI at a global level. More than 50% of all criminal investigations involve cross-border requests to obtain electronic evidence. That is why, in April 2018, following requests from the European Council and the Council, the European Commission proposed new rules aimed at making it easier and faster for authorities to access electronic evidence, regardless of where the data is located. According to the European Commission's initial proposal, "the new rules would allow judicial authorities in an EU country to directly request access to electronic evidence from any service provider providing services in the European Union and established or represented in another Member State" (Council of the European Union, 2024).

In the EU, regulatory developments were accelerated with the launch of the proposal for an AI regulation in April 2021. It sets out a comprehensive framework for the use of AI in various areas and is based on a risk-based approach, paying particular attention to applications considered to be "high-risk". The European Commission has therefore carried out consultations to obtain feedback from stakeholders, including academia, the private sector and

civil society, underlining the importance of respecting European values such as human dignity, freedom and justice.

To speed up the request for access and to eliminate the need for intervention by authorities in other Member States, two legislative proposals have been put forward: a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, which will allow authorities to access stored data regardless of its location, and a directive establishing harmonized rules on the appointment of legal representatives for the purpose of obtaining evidence in criminal proceedings, to ensure that all service providers operating in the EU have the same obligations regarding access to electronic evidence. On January 25, 2023, the Council confirmed the agreement with the European Parliament on the two legislative proposals.

In June 2024, the EU adopted the world's first AI rules (Idem). The Artificial Intelligence Law will become fully applicable 24 months after its entry into force, but certain parts will be applicable sooner:

- the ban on AI systems that pose unacceptable risks started to apply on February 2, 2025;
- the codes of practice will apply nine months after their entry into force;
- the rules on general-purpose AI systems that must comply with transparency requirements will apply 12 months after their entry into force;

Once the rules are adopted, the focus is on effective implementation and on the creation of regulatory bodies to oversee compliance. These organizations will have the role of checking that AI technologies comply with the rules and regulations set out in the legislation. As technology evolves, it is expected that regulations will continuously adapt.

The regulation of artificial intelligence (AI) in Romania is part of a broader effort at the European level, aiming to create a legislative framework that ensures the responsible and ethical use of AI technologies. In this context, Romania, as a member state of the European Union, aligns itself with legislative proposals and regulations issued by the European Commission (Idem). Ministries such as the Ministry of Research, Innovation and Digitalization collaborate with other institutions to develop policies and legal frameworks to support innovation in the field of AI, while protecting the rights of citizens.

1.2 Optimizing Criminal Investigations Through Technology

Integrating artificial intelligence into optimizing criminal investigations is a natural extension of streamlining the documentation process and improving the quality of judicial decisions. The principles outlined in the context of legal documentation also apply to the criminal field, where rapid access to relevant information, comprehensive data analysis, and process automation can transform the way investigations are conducted. For example, advanced artificial intelligence systems can facilitate rapid identification of evidence or witnesses by analyzing the context of events and correlating them with existing information.

Through machine learning algorithms, trends in recidivism and criminal behaviors could be identified, providing a solid basis for risk assessment and preventive measures. Real-time data analysis can also help prosecutors and investigators improve the quality of evidence, reducing human errors and inconsistencies in data collection and interpretation. However, the integration of artificial intelligence in this context is not without challenges, including ethical issues related to data privacy and the impact on individual rights. It is crucial that the systems used are transparent and operate within a framework that ensures respect for the fundamental rights of citizens. The implementation should also be accompanied by adequate training of personnel involved in investigations, thus ensuring not only the efficiency but also the legality of the criminal process. Therefore, the approach to integrating artificial intelligence into criminal investigation requires special attention to ensure not only the efficiency of the processes, but also the respect for the fundamental principles of justice.

2. The Conduct of the Criminal Proceedings and the Role of Evidence in the Proceedings

In criminal law, criminal trial represents "the activity regulated by law, carried out in a criminal case, by judicial bodies, with the participation of the parties, the main procedural subjects and other procedural subjects and which aims to establish in a timely and complete manner the facts that constitute crimes, so that any person who has committed a crime is punished according to his guilt and no innocent person is held liable" (Paraschiv et al., 2024, p. 1). In the context of criminal trial, the interdependence between the data relating to its conduct and the procedural phases is particularly important for understanding the mechanisms of law enforcement and guaranteeing justice. The criminal trial is structured into several phases, representing its divisions, each having specific roles and functions, and the data collected during these stages contribute to building a solid foundation for resolving criminal cases.

The initial stage, called criminal investigation, consists of carrying out investigative acts through which the competent authorities investigate the reported facts, having as their main objective the collection of evidence in order to restore the rule of law and sanction the guilty. Criminal investigations carried out at this stage include searches, hearings, identification of persons and objects, preservation of computer data, documents, removal of objects, expert assessments and findings, photography and fingerprinting, etc., with the role of clarifying the circumstances in which the crime was committed and determining the criminal responsibility of the persons involved.

Evidence plays a central role in all phases of the criminal process, serving to "establish the existence or non-existence of a crime, to identify the person who committed it, to know the circumstances necessary for the fair resolution of the case, as well as to find out the truth" (Paraschiv et al., 2024, p. 138). They are obtained in compliance with the principles of legality and fairness, being essential for substantiating the solution pronounced in court, thus ensuring both the protection of the fundamental rights of the persons involved and the conduct of a fair trial (Bitanga et al., 2018, p. 34).

3. Digital Proofs – Concept, Definition, Types

The digital revolution is profoundly reshaping all dimensions of social life, including the field of crime, which is no exception, "becoming an unavoidable reality, with a significant evolution and a development projection of the highest concern for law enforcement institutions" (Nucă, 2024). An increasing proportion of criminals use advanced technologies to design and execute various illicit activities. In this sense, judicial authorities are becoming increasingly dependent on electronic evidence in the process of identifying and sanctioning criminals, given the relevance and efficiency of this type of evidence in criminal proceedings. This change requires substantial adjustments in investigative methodology and in the application of legal norms, with an emphasis on the use of complex IT solutions that can increase the responsiveness of the criminal justice system (Council of the European Union, 2024).

3.1 Definition of digital evidence

Digital evidence constitutes "that information with probative value for criminal prosecution bodies and courts, that are stored, processed or transmitted by means of a computer system" (Romanian Information Technology Initiative and the Government of Romania, 2004, p. 72). Therefore, digital evidence has been defined as: "any information with probative value that is either stored, processed or transmitted in a digital format" (Ibidem). The European Council has also defined digital evidence as "data in electronic format used for the investigation of crimes and the prosecution of their perpetrators" (Council of the European Union, 2024).

3.1.1 Types of digital evidence

Digital evidence can be classified into: original digital evidence (which are physical elements and data about objects existing at the time of seizure) and duplicate digital evidence (which refers to an exact digital reproduction of all data about objects contained in an original physical item). Digital evidence includes computer evidence, digital audio evidence, digital video evidence, and evidence produced or transmitted by mobile phones, digital faxes, etc. One particularity of this type of evidence is that it is apparently not evident, as it is contained in the computer equipment that stores it. The forensic investigation team of computer crimes must be equipped with certain specific investigation equipment and software, in order to make this evidence available, tangible and usable. Another aspect is related to the fact that this evidence is very "fragile", in the sense that it can be easily altered or destroyed, by methods that are often within the reach of the perpetrators" (Moise, 2027).

The International Organization on Computer Evidence (IOCE), established in 1995 to provide international law enforcement agencies with a forum for the exchange of information on the investigation of computer crime and other computer-related forensic issues, has developed a series of principles (International Organization on Computer Evidence, 2020) in the field of digital evidence:

a. in the process of obtaining digital evidence, the actions taken should not be modified;

b. when it is necessary for a person to have access to the original digital evidence, this person should be forensically competent;

c. all activities related to the investigation, storage, examination or transfer of digital evidence should be fully recorded in writing, retained and available for review;

d. a person is responsible for all activities related to digital evidence, as long as it is in their possession;

e. any organization responsible for the investigation, access, storage or transfer of digital evidence is responsible for compliance with these principles.

Other organizations, such as the International Association for Computer Information Systems (IACIS), have provided a series of standards for the scientific examination of digital evidence (Shinder, 2002, p. 552):

- the original evidence should be preserved in a condition as close as possible to the condition in which it was found;
- an exact copy of the original should be made to be used for examination, so as not to destroy the integrity of the original;
- copies of data for examination should be made on data carriers, which do not have data stored on them; data carriers should be completely clean and checked for viruses and defects;
- all evidence should be marked, labeled and registered and a chain of custody should also be maintained, each step of the legal examination should be recorded in detail.

3.2 Legal efficiency through digital evidence and AI

The integration of artificial intelligence in the optimization of criminal investigations is closely linked to the use of digital evidence, which has become increasingly relevant in the current context of crime, especially in cases related to cybercrime or any activity involving digital technologies. Digital evidence, such as data from mobile phones, computers, social media accounts or communication networks, requires a systematic and efficient approach in order to be properly used in the judicial process.

Artificial intelligence can significantly improve the process of collecting and analyzing digital evidence through various automated methods. For example, machine learning algorithms can analyze large volumes of data to discover patterns or anomalies that could prove to be essential in investigations. They can be used to filter information and identify relevant data, thus reducing the time required for manual analysis. Artificial intelligence

systems can also facilitate the recovery of deleted or encrypted data, which is essential if criminals are trying to destroy evidence. The process of examining digital evidence can benefit from advanced image recognition and natural language processing tools, which can help extract and classify relevant information from text documents, emails or messages.

These innovations not only optimize the efficiency of investigations, but also contribute to increasing the quality of evidence brought to court. However, it is essential to take into account the challenges related to data confidentiality and the need to comply with legal rules on the protection of personal data. In addition, the ethical and theoretical challenges associated with the use of artificial intelligence in criminal proceedings must be addressed by establishing rigorous standards and clear regulations. In this sense, the integration of artificial intelligence in the optimization of criminal investigations through the use of digital evidence can significantly transform the way investigations are conducted, ensuring increased efficiency and better quality of the evidence collected. With responsible implementation and a well-defined ethical framework, these technologies can contribute to achieving more efficient and fair justice.

4. Traditional Evidence or Digital Evidence - Advantages and Disadvantages, Valorization

In criminal investigation, traditional evidence and digital evidence obtained through artificial intelligence, as previously mentioned, represent two essential categories that significantly influence the justice process. Traditional evidence, such as statements, material objects, documents, etc., is subject to strict admissibility rules and provides tangible clarity on the circumstances of the act. However, they are often vulnerable to subjectivity, and an example of this is statements that can be influenced by the emotions, states and personal perceptions of witnesses. In contrast, digital evidence has revolutionized the way criminal investigations are conducted, bringing many significant advantages.

One of the main benefits of digital evidence is the efficiency in processing and analyzing large volumes of data, which artificial intelligence can quickly identify and correlate, discovering patterns or anomalies that might go unnoticed in traditional analysis. This ability to filter information and provide relevant insights substantially improves the speed and accuracy of investigations. In addition, digital evidence is accessible and replicable, which allows for multiple analyses without affecting the original, thus ensuring the integrity of the evidence. Objectivity is also another major advantage: AI algorithms can eliminate human subjectivity, presenting the facts in a neutral and data-based manner, thus increasing their credibility and accuracy in court. However, to fully capitalize on these advantages, it is essential that the investigation is carried out in compliance with legal norms, and that technological expertise is combined with legal expertise. Thus, despite the challenges related to technological complexity and integrity risks, the integration of digital evidence into a modern judicial framework is crucial for ensuring efficient and fair justice, promoting a holistic approach in establishing the truth and enforcing the law.

5. Integration of Artificial Intelligence in Criminal Investigations – Accountability and Protection of Fundamental Rights

The discussion on the integration of artificial intelligence in criminal investigations cannot be approached without considering the possible violations of fundamental human rights. However, it is essential to underline that, when this technology is implemented in compliance with rigorous ethical principles and an appropriate legislative framework, its use can actually contribute to the protection and strengthening of these rights. Innovations brought about by artificial intelligence can significantly improve the efficiency of the judicial process, facilitating the identification of crimes, reducing the time needed to complete investigations and ensuring better management of evidence. This, in turn, contributes to the realization of the right to a fair trial and the protection of

individual rights before the courts (Criminal Procedure Code, General Part, Title I – Principles and limits of the application of criminal procedural law).

It is essential that the technology is used within a well-defined framework, which includes stringent regulatory measures that guarantee the respect and protection of fundamental rights. Implementing transparency protocols in the process of data collection and analysis is essential to prevent abuse and discrimination. It is also important that the use of artificial intelligence is subject to independent external oversight, which ensures accountability and protects the interests of individuals. These measures can help avoid situations in which fundamental human rights could be affected by ensuring a fair and transparent use of technology. By adopting a proactive approach, which integrates both technical and legal and ethical aspects, artificial intelligence can be transformed from a potential threat into a valuable tool. In this sense, technological advances should not be seen as a simple innovative solution, but as an opportunity to redefine and improve the justice system, which can thus become both more efficient and more respectful of the fundamental rights of citizens. Therefore, assuming collective responsibility regarding the use of these technologies is crucial to ensuring not only the efficiency of criminal investigations, but also social justice and the protection of fundamental rights.

6. Practical Aspects

6.1 The FBI and Internet Data Analysis

Recently, as manual examination of social media tends to be difficult, time-consuming, and arbitrary, making it more prone to errors, the FBI has integrated machine learning technologies, using artificial intelligence, into its investigative strategies to analyze and extract information from social media, with the goal of preventing and combating crime. According to the report "FBI: Social Media Analysis in Criminal Investigations," the agency uses algorithms to analyze large volumes of data, identifying behavioral patterns and correlations between suspect activities and criminality, which allows them to detect emerging threats and mobilize resources in a timely manner. Social network analysis (SNA) is becoming a valuable tool for law enforcement, improving the efficiency of investigations by systematically approaching large amounts of data about individuals and relationships. Using available data, police departments are structuring their examination of a criminal's social network in ways that were not previously possible, leading to increased crime clearance rates. This identifies human interactions that may facilitate illegal behavior, such as juvenile delinquency, illegal drug distribution, and international terrorism.

In January 2008, a pilot project was initiated at the Richmond Police Department (RPD), Virginia, to evaluate the use of SNA in crime investigation. The collaboration involved police officers, a sociologist, and a software designer, with the goal of analyzing crime data to understand violence between two groups of young men who were previously friends. The research team accessed the RPD's records management system to obtain information about criminal events and victim-offender relationships without directly interacting with detectives. Twenty-four persons of interest, labeled as "seeds," were used to construct networks based on their connections, resulting in 434 individuals and 1,711 ties.

The analysis revealed both positive (cooperative) and negative (hostile) ties between individuals, highlighting that disputes were often related to relationships with women. A centrality metric showed that certain individuals were essential to the network, confirming that gang units were directing their resources efficiently. Finally, the analysis identified key players influencing network dynamics, providing police with strategies for responding to the violence they detected.

Unforeseen administrative processes delayed the pilot project, resulting in late results, even though police had already resolved the conflict, validating the research team's analysis. Detectives said the SNA analysis had accelerated the resolution of the case. The analysts were

trained to use the SNA and, within two weeks, were applying the method to shooting and robbery incidents. In the shooting case, the analyst provided information about an associate of the suspect, helping to capture him. In another case, SNA analysis uncovered connections between suspects, facilitating the identification of a suspect involved in multiple robberies, and collaboration was enhanced through social diagrams.

Social network diagrams (SNDs) have become a crucial tool for the DPR in investigating the relationships between criminals and their associates. This method has improved communication between crime analysts and investigators, helping to increase case clearance rates and reduce violence.

Before SND training, analysts would create "star" networks by focusing on a person of interest and identifying direct connections. Later, through training, they learned to interpret the networks as a whole to obtain relevant information. By using SND in cases such as shootings and robberies, detectives have been able to identify critical connections between suspects and collaborators, facilitating the rapid resolution of cases. Access to SNA could have enabled other jurisdictions to uncover criminal connections earlier.

The case studies demonstrate the effectiveness of SNA in law enforcement strategies, revealing answers to complex questions about criminal motivation. The pilot project confirmed the contribution of SNA in elucidating violence between previously peaceful groups, improving collaboration between crime analysts and detectives. SNA helps solve institutional memory problems by providing a comprehensive picture of criminal networks, supporting both new and experienced analysts. Law enforcement agencies benefit from structured data to track changes in the network and identify gaps in data analysis.

Law enforcement agencies have made great strides in using technology to address complex crime problems. Social network analysis has proven to be effective in solving crimes and identifying persons of interest, bridging the gap between analysts and police officers. Robust technology in SNA provides rapid, actionable results, thereby improving police operations.

6.2 Analysis of digital evidence in terrorism cases

More and more criminals and terrorists are turning to technology to plan and commit crimes. As a result, authorities are increasingly relying on electronic evidence to detect and convict criminals. The EU is currently working on new rules to ensure a more efficient mechanism for cross-border access to electronic evidence, as 85% of criminal investigations involve digital data (Council of the European Union, 2024).

6.2.1 Europol's Data Analysis Initiative

Europol—officially the European Union Agency for Law Enforcement Cooperation—is the law enforcement agency of the European Union, established in 1998. It serves as the main centre for coordinating criminal intelligence and supporting EU Member States in their efforts to combat serious and organized crime, as well as terrorism (Europol, 2020; Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016).

In 2020, Europol introduced the "Smart Data" (SMART—Specific, Measurable, Attainable, Relevant, and Time-Bound—an acronym for the characteristics considered essential for the correct formulation of an objective: specific, measurable, attainable, relevant, and time-bound). "Smart Data" is an intelligent data mining solution that refers to a sophisticated software tool that uses advanced algorithms and machine learning techniques to automatically extract relevant information from various data sources. It intelligently identifies and extracts key data points, such as names, dates, and amounts from unstructured documents, enabling efficient data processing and analysis. By leveraging intelligent data mining capabilities, organizations increase efficiency, accuracy, and scalability in handling large

volumes of data) initiative, which uses artificial intelligence to facilitate the analysis of large amounts of data relevant to terrorism and organized crime cases.

The project integrates data from multiple sources, including social networks, government databases, information from law enforcement agencies, digital communications monitoring and open sources (OSINT—Open Source Intelligence involves the precise research of open sources of information, from the press and the internet, to libraries and bookstores). It addresses both structured data (e.g., tables, databases) and unstructured data (e.g., text, images, videos) to obtain a complete picture of suspicious activities. It uses machine learning techniques to identify patterns and anomalies in the data, with algorithms able to recognize suspicious behaviors and provide clues about possible illegal activities. It implements predictive models that help anticipate and prevent events carried out by terrorist groups or criminal organizations and also provides visual tools that allow analysts to explore the complexities of data through graphs, charts and maps, helping to identify connections between different entities and events and creating interactive dashboards that summarize data in easy-to-understand ways, allowing real-time tracking of suspicious activities.

The project involves collaboration between different law enforcement agencies, international organizations and academic institutions to maximize the use of available resources and expertise and facilitates the exchange of relevant information between agencies, contributing to a more coordinated and effective response to threats. The project includes strict compliance measures with data privacy and human rights regulations, ensuring that the technology is used in an ethical manner.

6.2.2 Paris Terrorist Attacks

The Paris terrorist attacks, carried out on 13 November 2015, were a coordinated attack on the French capital, targeting both innocent civilians and international symbols of freedom, democracy and cultural diversity. These attacks, planned by the terrorist group ISIS (The Islamic State, alternatively: Islamic State of Iraq and the Levant or Islamic State of Iraq and Syria, abbreviated: IS, SI, ISIL and ISIS), a Sunni Salafist insurgent terrorist group affiliated with al-Qaeda, active in Iraq and Syria and an Islamic state (proclaimed caliphate) unrecognized by international law, resulted in the loss of at least 130 lives and the injury of over 400 others, constituting one of the deadliest terrorist attacks in Europe in recent decades (Europol, 2015).

The attacks were classified as murders against humanity under the principles of international criminal law. According to the Rome Statute of the International Criminal Court, attacks on civilians constitute a serious violation of international humanitarian law and human rights. Following the attacks, a state of emergency was declared in France, with the aim of strengthening security measures and preventing similar incidents. The French legislature has adopted a series of legislative amendments to expand the powers of law enforcement agencies, including by facilitating the interception of communications and expanding surveillance capabilities. Under European law, victims of terrorism have the right to compensation and assistance, and member states are obliged to provide them with adequate protection.

The European Union countries have also agreed on stricter security measures and cooperation in the field of intelligence, in order to prevent future terrorist attacks, which is why, after the attacks, French authorities and international security agencies have begun to resort to advanced technologies, including artificial intelligence, to facilitate the investigation and prevention of future attacks.

Machine learning algorithms and natural language processing were implemented to analyze digital data (evidence) extracted from suspects, including messages on encrypted communication platforms and activity on social networks. Artificial intelligence technologies capable of handling large volumes of data were essential for the investigative work. These allowed authorities to quickly identify connections between suspects, track communication

patterns and analyze suspicious behavior on social networks. This type of analysis contributed to the discovery of terrorist support networks and the prevention of imminent attacks.

Conclusions

The implementation of a dedicated AI system in the Romanian judicial system represents a significant opportunity to modernize and streamline the act of justice. The success of the implementation depends on the systematic approach to the identified challenges and the close collaboration between all actors involved.

In the context of the diversification of types of digital evidence, the development of a legal framework and standards for the collection, analysis and presentation of evidence becomes imperative. Adherence to international best practices and coordination of regulations at the European level can improve the quality and credibility of digital evidence in courts. "In this digital age, the relationship between AI and the judiciary increasingly resembles a complex dance – sometimes in perfect sync, sometimes stepping on each other's toes. And while technology promises to be a reliable partner in the courtroom, we should remember that justice, like love, cannot be reduced to an algorithm. So as AI makes its way into code and case law, perhaps we should make sure we don't turn Themis, the goddess of justice, into a robot who simply processes data – after all, she carries the scales of justice in her hands, not in integrated circuits". As crime becomes increasingly sophisticated, the challenges of using artificial intelligence in criminal investigation will intensify. Thus, proactive approaches, based on case studies and examples of good practice, will be essential in developing innovative and effective solutions in combating crime.

This paper therefore provides a comprehensive vision of how the integration of AI can transform the modern judicial process, while emphasizing the importance of regulation and respect for fundamental rights. The responsible implementation of these technologies has the potential to improve not only the efficiency of investigations, but also the credibility and fairness of the judicial system as a whole (Goga, 2025).

References

Bitanga, M., Franguloiu, S., & Sanchez-Hermosilla, F. (2018). *Guide to procedural rights of suspects and defendants: The right to information and the right to translation and interpretation*. Magic Print.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*.

Council of Europe. (1950). *European Convention on Human Rights*.

Council of the European Union. (2024). *Better access to e-evidence to fight crime*. https://www.consilium.europa.eu/ro/policies/e-evidence/

Criminal Procedure Code. (n.d.). *General part: Principles and limits of the application of criminal procedural law*.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. (2002). *Official Journal of the European Union*, L201/37.

Europol. (2015). *The terrorist threat in the European Union: A joint report on terrorism*.

Europol. (2020). *Internet organised crime threat assessment (IOCTA) 2020*. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Franguloiu, S. (2023). Principles for the use of artificial intelligence (AI) in the judiciary as derived from the European ethics charter: Justice efficiency and limitations. *Bulletin of Transilvania University of Braşov, Series VII: Social Sciences. Law*, 16(65), 1. https://webbut.unitbv.ro/index.php/Series_VII/article/view/6939/5301

Goga, A. S. (2025, January 27). *Utilizarea inteligenței artificiale în juridic și judiciar – avantaje și dezavantaj*. *Juridice.ro*. https://www.juridice.ro/768913/utilizarea-inteligentei-artificiale-in-juridic-si-judiciar-avantaje-si-dezavantaje.html

International Organization on Computer Evidence. (2020). *International principles for digital evidence*. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#IOCEInternationalPrinciples

Johnson, J., Reitzel, J. D., Norwood, B., McCoy, D., Cummings, B., & Tate, R. (2013, March 5). *Social network analysis: A systematic approach for investigating*. *FBI Law Enforcement Bulletin*. https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating

Moise, A. C. (2017). Aspecte referitoare la administrarea probelor în cazul infracțiunilor informatice. *Acta Universitatis George Bacovia. Juridica*, 6(2), 513–528.

Nguyen, T. H., & Vola, K. (2020). Artificial intelligence in the courtroom: The future of justice. In *Artificial intelligence for the legal profession: An overview* (pp. 201–225). Springer.

Niță, N., Hegheș, N. E., & Apreutesei, C. (2025). Brief considerations on the impact of artificial intelligence on forensic science, silent and powerful ally of justice. *Romanian Forensic Scientists Association*, 26(3), 143.

Nucă, N. (2024, January 29). *Criminalitatea organizată. Tehnici de prevenire și combatere*. *Juridice.ro*. https://www.juridice.ro/722637/criminalitatea-organizata-tehnici-de-prevenire-si-combatere.html

Organisation for Economic Co-operation and Development. (n.d.). *AI principles: Principles and guidelines for the responsible development and use of artificial intelligence*. https://www.oecd.org/en/topics/policy-issues/artificial-intelligence.html

Paraschiv, C.-S. (Coord.), Teodorescu, M.-G., & Nicolescu, A. S. (2024). *Drept procesual penal. Partea generală. Note de curs* (6th ed., rev. & updated). Hamangiu.

Predictive policing: Review of benefits and drawbacks—An assessment of the use of machine learning technologies in law enforcement, including contextual analysis of social networks. (n.d.).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (2016). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Romanian Criminal Code. (2009). *Law no. 286/2009 on the Criminal Code*. Official Gazette of Romania No. 510/2009.

Romanian Information Technology Initiative & Government of Romania. (2004). *Introductory guide for the application of legal provisions regarding cybercrime*. http://www.ritiinternews.ro/ro/ghid.htm

Social network analysis in criminal justice: A review—Article providing an overview of social media analysis in the context of criminal justice. (n.d.).

UNESCO. (2021). *Tribute to the chairperson of the executive board (41 C/PLEN/DR.3)*. https://unesdoc.unesco.org/ark:/48223/pf0000379926