RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
June 5-6,2025

DOI: 10.5281/zenodo.16218052

Advantages of Using AI in the Criminal Prosecution Phase for Digital Evidence Analysis

Carmen Silvia Paraschiv

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

Abstract: The study analyzes the use of artificial intelligence (AI) in the criminal prosecution phase, with a focus on the analysis of digital evidence. It presents the types of AI technologies used, their concrete applications in crimes investigation, as well as the benefits and the technical, legal, and ethical risks. Relevant international examples are highlighted and directions for regulation, professional training and standardization are proposed. The conclusion emphasizes the need for a balance between technological innovation and the guarantee of fundamental rights in a fair criminal trial.

Keywords: Artificial Intelligence, Digital Evidence, Criminal Prosecution, Digital Forensics, Criminal Justice, Algorithmic Transparency, AI Audit

1. Introduction

In an era marked by a profound and continuous digital transformation, the use of artificial intelligence (AI) in the criminal justice system is gaining increasing strategic relevance. This trend reflects not only exponential technological advances but also the need for judicial institutions to adapt to the complexity of new forms of crime, especially those carried out in cyberspace. In this context, AI is no longer perceived as a simple technological innovation but as a potentially transformative tool capable of redefining the dynamics of criminal investigations and supporting decision-makers in the law enforcement process.

Among the significant areas in which AI is proving its usefulness is the analysis of digital evidence, an essential component of contemporary criminal investigation. With the massive digitization of communications, social interactions and economic activities, digital evidence (such as emails, media files, data stored in the cloud or metadata of electronic devices) has become ubiquitous in criminal cases. They provide valuable information for reconstructing facts, identifying participants and proving criminal intent, but their volume and complexity require the use of advanced data processing and interpretation technologies.

The integration of AI in this procedural stage thus allows for a significant streamlining of the activity of criminal prosecution bodies, by automating laborious tasks, reducing analysis times, quickly identifying behavioral patterns and extracting relevant information from large masses of unstructured data. At the same time, it contributes to increasing the precision in the decision-making process, reducing the risk of human error and providing an objective perspective on the available evidence.

The purpose of this study is to systematically analyze the concrete applications of artificial intelligence in the analysis of digital evidence in the criminal prosecution phase, by highlighting the functional advantages brought by these technologies, as well as the associated legal and ethical risks and limitations. In this sense, the study is part of the broader efforts of the academic and legal community to understand and regulate in a coherent and responsible manner the interaction between technology and the criminal justice system (European Union Agency for Fundamental Rights, 2020).

2. Theoretical and conceptual framework

2.1. Artificial intelligence: definitions, types and evolution

Artificial intelligence (AI) is an interdisciplinary field located at the intersection of computer science, mathematics, neuroscience and formal logic, aiming to develop systems capable of

reproducing or simulating behaviors associated with human intelligence, such as learning, reasoning, decision-making and pattern recognition. Definitions of AI have evolved with technology, from the design of simple rule-based expert systems to advanced machine learning and deep neural networks that can analyze massive amounts of data and generate complex predictions.

Among the most widely used types of AI in forensic analysis are:

- Machine learning, which allows systems to improve their performance based on experience gained from data;
- Natural Language Processing (NLP), a technology that allows the interpretation and generation of human language, is essential in the analysis of conversations and electronic documents;
- Computer vision, which refers to the ability of systems to interpret and analyze visual information, such as images or video recordings.

These technologies, used in isolation or combination, form the core of modern AI applications in justice, with the potential to accelerate evidence analysis processes and provide investigators with new insights into criminal dynamics (Russell & Norvig 2021).

2.2. The criminal investigation phase in the Romanian criminal trial

In Romanian criminal procedural law, the criminal investigation phase constitutes the preliminary stage of the criminal trial, in which the criminal investigation bodies, under the supervision and leadership of the prosecutor, are responsible for identifying the crime, its perpetrators and collecting relevant evidence in order to establish the judicial truth (Russell & Norvig 2021). The fundamental purpose of this phase is to carry out an objective, complete and legal documentation of the facts, so that the court can subsequently pronounce a correct and thorough solution.

This stage involves a multitude of specific activities, such as: hearing witnesses, computer searches, collecting evidence, intercepting communications, forensic expertise, all of which have the role of building a coherent image of the investigated act. In this context, the use of AI technologies supports both the speed and accuracy of the evidentiary process (López 2022).

2.3. Digital evidence: definition, typology and legal regulation

Digital evidence is information generated, stored, transmitted or processed by electronic means, which can be used to prove the existence of a relevant fact in a criminal trial. This may include electronic messages, images, video recordings, audio files, internet browsing history, location data, conversations on messaging applications, system files or metadata associated with these elements (Romanian Criminal Procedure Code, art. 285 et seq.).

In Romanian law, the legal framework regulating the use of digital evidence is represented mainly by the Criminal Procedure Code, but also by the special legislation on computer crime (Law no. 161/2003, Law no. 64/2004), as well as by European regulations on data protection and procedural rights in criminal proceedings. The legality of obtaining, preserving and using this evidence is essential to guarantee a fair trial, in accordance with the principle of legality and respect for all fundamental rights.

2.4. Digital Forensics and its role in criminal investigations

Digital forensics, or digital forensics, is the branch of forensic science that deals with the identification, collection, examination and interpretation of electronic evidence, in order to present it to the competent authorities (Maras, 2015). The digital forensics process involves a rigorous methodology, starting from preserving the integrity of the data, passing through technical analysis and continuing with the detailed documentation of the expert's conclusions.

The role of this field is crucial in the investigation of modern crimes, such as computer fraud, distribution of illicit materials, cyber-attacks or terrorist activities carried out online. At

the same time, digital evidence can constitute evidence in classic criminal cases (murder, human trafficking, etc.), since most suspects use electronic devices in their daily lives.

2.5. Types of AI used in digital evidence analysis

In digital evidence analysis, various types of artificial intelligence are used synergistically to optimize the investigative process. Machine learning algorithms are trained to recognize suspicious patterns in files, communications or online behaviors, being able to automatically identify relevant documents from large volumes of data.

Natural language processing technologies allow the analysis of written or transcribed conversations, identifying relevant expressions, intentions, emotions or inconsistencies in statements. Computer vision is also used to analyze screenshots, images or video recordings extracted from devices or surveillance systems, facilitating facial recognition, object or place identification (Wachter, Mittelstadt & Floridi, 2017).

The integration of these technologies into a secure and controlled legal framework is essential to ensure the validity of evidence and the protection of the fundamental rights of the parties involved (Casey, 2011).

3. Study methodology and concrete applications of Artificial Intelligence in digital evidence analysis

The study has a theoretical-applied nature, based on the analysis of specialized literature, legal regulations and examples of international good practices. Academic sources, technical reports and official documents in the field of justice and technology were analyzed.

The implementation of artificial intelligence (AI)-based technologies in digital evidence analysis offers a diverse range of practical applications, which significantly contribute to the efficiency and accuracy of criminal investigations. These applications not only optimize traditional processes of identifying and classifying evidence, but also enable innovative approaches that would previously have been impossible to achieve in a reasonable time frame or with limited human resources.

3.1. Automatic recognition of relevant content

One of the most useful functionalities of AI in digital analysis is the ability to identify specialists who can detect sensitive terms, key phrases or standardized legal formulas, thus contributing to accelerating the process of selecting and prioritizing relevant evidence (López, 2022). In this sense, AI works as an intelligent filter, considerably reducing the volume of data that investigators have to analyze manually and at the same time improving the quality of the evidence.

3.2. Analysis of conversations in messages and emails

Natural language processing (NLP) technologies allow the semantic and contextual interpretation of the content of electronic conversations, such as emails or instant messages. NLP algorithms can distinguish not only the general topic of the discussion, but also the intentions, emotions or tone of the users, providing important clues about the possible criminal intentions of the suspects (Chatterjee & Dethlefs 2020). This capability is particularly relevant in cases of conspiracy, fraud or trafficking, where coded or indirect language can conceal illegal activities.

3.3. Metadata extraction and timeline reconstruction

Metadata associated with digital files – such as creation date, geographical location, author, device used – can provide essential information in the investigation of a criminal act. AI algorithms can extract this data in an automated manner and integrate it into a coherent timeline of events, thus facilitating the precise reconstruction of causal and evidentiary sequences (Casey, 2011). This function is vital in documenting the chain of actions taken by a participant and in establishing key moments in the commission of the crime.

3.4. Digital file classification

The automatic classification and organization of digital files is another fundamental application of AI in the field of digital forensics. Intelligent systems can analyze the content of files and determine their typology (text, image, video, audio), as well as their relevance in relation to the investigation hypothesis (Maras, 2015). Through this function, evidence is prioritized according to the degree of priority, which allows for a more efficient use of time and resources available for the investigation.

3.5. Detection of altered documents

Alteration of digital files or electronic documents is a common practice in cybercrime and beyond. Computer vision technologies, combined with forensic watermarking or digital signature analysis methods, are capable of detecting unauthorized modifications, overwrites, graphic forgeries or structural inconsistencies in documents (Garfinkel, 2010). This application strengthens the evidentiary function of digital documents, providing a greater degree of confidence in their authenticity and protecting the integrity of the evidence presented in court.

4. Challenges and limitations of the use of Artificial Intelligence

Although the use of artificial intelligence in criminal proceedings promises multiple benefits, such as increasing the efficiency of investigations and improving the quality of decisions, it is accompanied by a number of significant challenges and limitations. These concern both technical and legal aspects, as well as profound ethical and social implications. In the absence of a well-founded normative and technological framework, the uncontrolled use of AI in criminal proceedings can generate considerable risks for the fundamental rights of the persons under investigation.

4.1. Technical issues

From a technological point of view, AI systems are susceptible to algorithmic errors, false positive or negative results, as well as to limitations of the training data used in the development of predictive models. The quality of predictions and interpretations generated by AI directly depends on the volume, accuracy and diversity of data introduced into the system. If this data is incomplete, biased or irrelevant, the algorithm can produce erroneous conclusions, negatively influencing legal decisions (Amodei et al., 2016). Systems can also become unstable in the face of unforeseen contexts, which raises serious reliability issues in criminal proceedings.

4.2. Legal issues

The use of AI in criminal proceedings raises multiple legal issues, especially regarding the admissibility of automatically processed evidence. In Romanian criminal law, evidence must comply with the requirements of legality, loyalty and relevance, and the introduction of results generated by AI systems into the file can be challenged if it is not clear who controlled the process, how the algorithm was configured and to what extent the results are verifiable (Surden, 2019). In addition, the lack of a specific legislative framework for the use of AI in the field of justice complicates the integration of these technologies in practice, generating legal uncertainty and difficulties in guaranteeing a fair trial.

4.3. Ethical issues

The risk that technology will be used in a disproportionate or invasive way. Digital evidence often contains sensitive information about an individual's personal behaviour, social relationships and preferences, and its analysis by an automated system involves risks of intrusion into the sphere of intimate life (European Union Agency for Fundamental Rights, 2020). There is also the danger

that the data collected will be used outside the original investigative purpose or stored without the consent of the person concerned.

4.4. Lack of algorithmic transparency

Another major limitation is the opaque nature of many AI systems, which function as "black boxes", i.e. they generate results without allowing a clear understanding of how these results were obtained. This lack of transparency makes it difficult to justify conclusions in court, affecting the principle of adversarial proceedings and the right to defence (Wachter, Mittelstadt & Floridi, 2017). In addition, the lack of algorithmic auditing mechanisms and user-friendly explanations can lead to distrust in the technology and to questioning the validity of these systems in the legal sphere.

5. Reference cases and good practices

The integration of artificial intelligence into judicial systems has experienced uneven development globally, reflecting both differences in legal traditions and the levels of technological maturity of different states. However, there are some examples of good practices that can serve as benchmarks in outlining a framework for the ethical, efficient and legal use of AI in criminal proceedings, in particular with regard to the analysis of digital evidence and algorithmically assisted judicial decision-making.

One of the most discussed cases is that of the COMPAS system (Correctional Offender Management Profiling for Alternative Sanctions), implemented in the United States of America to support courts in assessing the risk of recidivism of defendants at the time of sentencing or parole decisions (Angwin et al., 2016). Although this system offers a standardized and rapid method of analysis, it has been criticized for the lack of transparency of the algorithm and for the possible perpetuation of systemic biases based on race or socio-economic status (Dressel & Farid, 2018). However, COMPAS remains a relevant example of how AI can influence judicial processes and has triggered important international debates on the ethics and responsibility of using algorithmic technologies in justice.

At the European level, projects such as ROXANNE (Real-time network, text, and speaker analytics for combating organized crime), funded by the European Union through the Horizon 2020 program, stand out. It aims to develop integrated technological solutions that allow the automatic analysis of criminal communications by combining voice recognition, natural language processing and social network analysis technologies (ROXANNE Project, 2021). The project represents an advanced example of cooperation between judicial authorities, researchers and technology companies, in order to support the fight against organized crime through AI-based tools.

As for Romania, although the implementation of AI in judicial activity is at an early stage, a number of initiatives for the digitalization of justice are observed, such as automated case law portals, electronic files or automatic transcription systems of court hearings. These tools can represent a solid basis for the subsequent integration of AI components, especially in the field of digital evidence management and analysis (European Commission, 2020). At the same time, the European Commission encourages Member States to adopt national AI strategies that also include justice-related aspects, which offers Romania the opportunity to develop a coherent framework for the use of these technologies in the future.

6. Development prospects and recommendations

As technologies based on artificial intelligence become increasingly present in judicial activities, it is necessary to develop a clear normative and operational framework to guide the use of these tools in a responsible, ethical and efficient manner. In the absence of coherent regulation, the application of AI in justice risks generating more problems than solutions, including legal

conflicts, inequalities in the treatment of litigants and the loss of public confidence in the impartiality of the criminal justice system.

A first priority direction is the explicit regulation of the use of AI in the context of criminal proceedings, both in terms of the admissibility of evidence generated or processed algorithmically, and the protection of personal data and the procedural rights of defendants (European Commission, 2020). This regulation should include transparency standards, criteria for scientific validation of the algorithms used and clear mechanisms for judicial control.

In parallel, continuous professional training of anchors and technical experts in digital skills and the use of emerging technologies is essential. Only by thoroughly understanding the functioning and limitations of these tools can their rigorous and conscious application in judicial activity be ensured (European Commission for the Efficiency of Justice, 2021). The judiciary must also be supported in interpreting and evaluating the results obtained by automated means, in order to be able to correctly assess their evidentiary value. At the same time, it is recommended to develop standardized protocols for integrating AI into the workflow of criminal prosecution, in particular with regard to the analysis of digital evidence. These protocols should clearly define the operational steps, the responsibilities of the actors involved and the conditions for the use of algorithmic technologies, in order to guarantee compliance with the procedural and deontological principles of criminal law.

In order to ensure transparency and the proper functioning of AI systems, it is necessary to implement algorithmic audit mechanisms, through which the performance, correctness and lack of bias of the algorithms used in justice are periodically assessed (Raji & Buolamwini, 2019, 429-435). Such audits contribute not only to improving the quality of technologies, but also to strengthening public trust in decisions made with the support of AI.

Last but not least, it is necessary to promote inter-institutional partnerships between public actors (judicial institutions, regulatory authorities, universities) and the private sector (developers of technological solutions, cybersecurity companies), with a view to a sustainable and ethical development of AI applications in the criminal field. Such collaborations can contribute to the creation of integrated platforms, the exchange of best practices and the harmonization of technical standards with legal requirements (Raji & Buolamwini, 2019, 429-435).

Therefore, the development and application of AI in the analysis of digital evidence should not be just a matter of technological progress, but a multidisciplinary strategy, in which law, ethics and technology intersect to support a fair, efficient and citizen-oriented act of justice.

7. Conclusions

Artificial Intelligence (AI) is emerging as one of the most promising technological innovations applicable in the field of criminal justice, especially in the context of digital evidence analysis. This trend is fueled by the need to deal with an increasing volume of electronic data, the growing complexity of cybercrime and the requirement for a rapid, rigorous and rule-of-law-compliant institutional response.

Within the criminal prosecution phase, the integration of AI offers substantial opportunities for optimizing the process of collecting, selecting and interpreting evidence, contributing to streamlining investigative efforts and reducing the time needed to analyze relevant information. Machine learning, natural language processing and computer vision technologies allow not only a better organization of evidence, but also the discovery of correlations or clues that could be overlooked in an exclusively human analysis (Casey, 2011).

However, the widespread adoption of these tools must be carried out with caution and under the authority of a solid legal and ethical framework. Without adequate guarantees regarding algorithmic transparency, accuracy of results, protection of personal data and respect for procedural rights, the use of AI risks undermining public trust in the justice system and

directly affecting the right to a fair trial (European Union Agency for Fundamental Rights, 2020). Thus, the potential benefits of AI cannot be dissociated from the institutional responsibility to guarantee human control, auditability and fairness of decisions based on algorithmic systems (European Union Agency for Fundamental Rights, 2020).

In conclusion, the implementation of AI in the analysis of digital evidence represents an inevitable and necessary direction in the context of the digital transformation of criminal justice. However, the balance between technological innovation and respect for the fundamental values of criminal law must remain an absolute priority. Only through a multidisciplinary approach, based on collaboration between technology experts, lawyers and decision-makers, can a judicial system be built that is intelligent, but at the same time fair, transparent and humane.

References

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety*. arXiv:1606.06565.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Academic Press.

Chatterjee, S., & Dethlefs, N. (2020). Explainable Artificial Intelligence for Natural Language Processing: A Survey. *arXiv preprint arXiv:2004.14592*.

Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1), eaao5580. https://doi.org/10.1126/sciadv.aao5580

European Commission for the Efficiency of Justice (CEPEJ). (2021). *European Ethical Charter on the use of Artificial Intelligence in Judicial Systems*. Council of Europe.

European Commission. (2020). *White Paper on Artificial Intelligence – A European approach to excellence and trust*. Brussels: European Commission.

European Union Agency for Fundamental Rights. (2020). *Getting the future right – Artificial intelligence and fundamental rights*. Publications Office of the EU.

Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73.

López, A. (2022). *Artificial Intelligence and Criminal Justice*. Springer.

Maras, M.-H. (2015). *Computer forensics: Cybercriminals, laws, and evidence*. Jones & Bartlett Learning.

Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, 429–435.

Romanian Criminal Procedure Code (2010). Law no. 135/2010 on the Code of Criminal Procedure, published in the Official Gazette of Romania, Part I, no. 486 of July 15th, 2010, as subsequently amended and supplemented.

ROXANNE Project. (2021). *Combating Organized Crime through AI Technologies*. https://www.roxanne-euproject.org

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

Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1305–1337.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*, *2*(6), eaan6080

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99.