ARTIFICIAL INTELLIGENCE - RISK OR SECURITY IN FORENSICS?

DOI: https://doi.org/10.53486/dri2026.88
UDC: 343.98:004.8(4)

Roxana Mihaela MOISOIU
U.S.P.E.E. „ Constantin Stere"
Chișinău, Republic of Moldova
Email : roxana_moisoiu@yahoo.com
ID orcid 0009-0005-0515-0432
Prof. Colegiul German „Goethe"
Bucharest, Romania

Abstract: *Artificial intelligence influences the areas of our lives, including forensic investigations. The accelerated development of cutting-edge technologies has brought a series of advantages but also vulnerabilities and risks.*
Excessive dependence affects several aspects of the criminal process.
The paper analyzes the duality of artificial intelligence in the forensic process, highlighting both its role as a security and efficiency tool for investigations, as well as its potential for risk in the context of cybercrime and ethical and legal challenges, aiming to identify a balance between the advantages of technology and the respect for fundamental rights through responsible use in forensic activity.
The theme is current through the novel elements addressed. The article represents a point of view on AI and its use.
The development of artificial intelligence generates new forms of crime, for which it is necessary to have a clear legislative framework, ethical control mechanisms and interdisciplinary collaboration between specialists in law, computer science, sociology and cybersecurity.
The future of all humanity depends on international cooperation in combating new forms of crime and finding a set of unanimously accepted norms regarding the use of AI.

Keywords: *AI, forensics, algorithms, high-tech systems, risk, vulnerability*

JEL: K14

Introduction

In the context of globalization, the convergence between forensics and Artificial Intelligence is currently recording devastating consequences. Both in the field of forensics, when we mention the investigation and research of crimes, and in the field of jurisprudence, when judges base their final conviction decisions on judicial practice in the field and related legislation - we can state through pertinent arguments that we are witnessing an AI intrusion. We refer to AI intrusion because it produces both advantages and disadvantages, respectively risks in the situation where the judge's decision is based only on the algorithms used by AI.

Most criminal cases and not only in the situation of high-risk crime - but organized crime also - there are entire volumes of documents (statements, expert reports, judicial practice, jurisprudence) that would require unlimited time for analysis and research.

In Romania, in the Caritas (File nr. 138/85/2023) case, the volumes of the files reached several tons, and could be transported from one court to another by at least 4 trucks. At that time, the court hearings were many and over long periods of time, the process being delayed for several years, precisely because the competent authorities solving the case needed tens of thousands of hours for reading.

In forensic research, AI increases efficiency and reduces the time required to obtain significant results, both when drafting reports to terminate criminal prosecutions by judicial bodies and when drafting indictments by the court.

Modern systems identify connections that are impossible to observe in the traditional way, facilitating investigations. An example of this would be facial recognition algorithms, real support in identifying suspects. AI has developed analysis tools that investigate cybercrime and even cross-border crimes.
Forensic science is the one that has recorded greater performance by resorting to AI. It is known that the use of AI tools was first used in police work, namely forensics, by the police in Avon and Somerset (UK). At that time, SOZE as an AI tool was created to quickly analyze huge volumes of data. For example, extremely complex cases have been solved in just 30 hours with the help of AI. And if a person had to go through the same volume of data, it would have taken him 81 years. The tool used by AI uses machine learning algorithms, so that enormous amounts of data and information from files, video recordings, witness statements, reports and expertise - can be correlated by SOZE which can scan finding patterns, connections, and new identification leads in record time.
Beyond SOZE's use of facial recognition functions through which police work gains both time and field of action of great importance is the linguistic analysis and statistical (In Roxana Moisoiu's doctoral thesis, which is in manuscript.) predictions used by AI in various fields of research. In the research carried out to establish the causes of crime committed against property and people, the use of AI by documenting national, European, international statistics has led to the development of effective syntheses in research. But the decision-maker regarding the proposals for *lege ferenda* was neither the algorithm nor SOZE, but the one who took the scientific approach, that is, the researcher.
The limits of AI, beyond its undeniable benefits, must consider those aspects that refer to ethics, that is, to the rules and principles that must be respected in scientific research in the context in which cybersecurity risks appear quite frequently.
Content.AI technology both in forensics, when we mention the management of a huge volume of data, and in the practice of courts of law (by reporting decisions to the entire jurisprudence) - gives rise to controversies related to the emergence of possible risks, both of a cybernetic and ethical nature. Thus, reference can be made to those violations of personal data, in the situation where AI systems through manipulation generate false information about individuals, as well as about their past or present.
It is known that the EU, through its digital single market, has become known for the use of AI since 2010. For 10 years, violations of personal data and more have been recorded.
The consequences produced in the related field led the European Commission to adopt a White Paper in 2020. In the legal doctrine, both the civil and criminal liability of the legal person from the perspective of AI have been debated.
Considering the provisions of art. 535 of the Criminal Code, electro-magnetic waves, energy produced, captured and transmitted, things embedded in a building (elevator, escalators), water, electricity and gas sewage installations, certainly transcend the limits to AI.
From the perspective of criminal law related to AI, we can refer to the report initiated by the European Parliament in 2017 in which it discussed the recognition of the legal personality of robots as electronic persons, thus in the Criminal Code, in paragraph 1.3 of article 535, the liability of legal persons is regulated.
In Romania, the Criminal Code incriminates computer fraud (art. 249 of the Criminal Code), illegal access to an information system (art. 360 of the Criminal Code), unauthorized transfer of computer data (art. 362 of the Criminal Code) and so on. There is Chapter VI of Title VII of the Special Part of the Criminal Code dedicated to computer crimes, but artificial intelligence is not clearly specified.
It is obvious that the use of AI in the legal field has numerous advantages, but it should be noted that there are also risks and vulnerabilities.
One of these is the risk of algorithmic errors, because there is the possibility that the training data is incomplete or erroneous and then incorrect conclusions are generated (algorithmic bias). In forensics, an algorithmic error can influence the criminal process, by altering the presumption of innocence, can lead to judicial errors and even to limiting the freedom of the people involved.

Given the fragility of forensic systems based on AI, they can easily be the target of cyber-attacks that can manipulate databases or compromise digital evidence, using a spectrum that is difficult to detect. Evidence created or interpreted only with AI affects the fundamental principles of a fair trial through the lack of transparency.
Because AI uses sensitive information related to the processing of personal data, it is necessary to respect the right to privacy and the protection of this data.
Establishing legal liability for errors and vulnerabilities that occur is currently the prerogative of users and institutions that use these AI tools.
If we were to talk about the fact that AI can imitate people's voices or resemble audio files with human voices, we find that the systems have evolved and that they can produce vulnerabilities or risks through improperly used progress.(American science fiction writer Issac Asimov evokes, in the short story Runaround, the story of a robot designed and created by engineers Gregory Powell and Mike Donavan) Another possible risk is given by forms of permanent surveillance that are in antithesis to the principles of the rule of law and ethics.
Analyzing ethics from the perspective of AI, we must relate to the rules and moral principles that support the development, implementation and use of AI techniques. The current prospects of cutting-edge technologies in all fields of activity offer both advantages by improving working times and performance itself, providing personalized solutions for everyone.
Thus, in the field of medicine, the use of AI gives research the possibility of diagnosing conditions in minimal real time or performing surgical interventions with the help of the Da Vinci robot - a cutting-edge technology with minimally invasive risks and with a rate close to a minimum mortality limit. It should not be forgotten that the Da Vinci robot is directed by a human. who, using the precision of AI, reaches performance in interventional medicine. (especially in the case of incurable diseases). The performance obtained by using AI algorithms cannot be ignored, however.
Often its cost is at the expense of ethical rules that are not respected under the impact of AI. That is why UNESCO, EU, and Council of Europe documents provide the necessary legal framework and recommendations mandatory for all AI users, but equally for AI creators. And yet, even if AI through the algorithms used becomes essential for research performance, we must not ignore or forget the fact that only a human being can be creative, intuitive, emotional, and passionate, and AI through robotization only offers speed and precision in analysis and diagnosis.
To mitigate risks, it is necessary to have special legislation and implement preventive technical measures. Algorithms can be audited through periodic verification, data can be encrypted, and secure backups can be made to detect intrusions. All these aspects can be achieved by developing clear standards regarding the limits of AI use.
Human experts must always validate the final decisions, in all situations where AI algorithms are used.
Jeoffrey H, considered the godfather of AI, states that when an entity becomes smarter and more powerful than us, the hierarchy is reversed. The issue of ethics from the perspective of AI technologies must be understood, implemented and respected precisely because any violation of it violates fundamental rights.
The dream of creating humanoid robots has always existed. It is known that the "spring of artificial intelligence" dates to 1942. (American science fiction writer Issac Asimov evokes, in the short story Runaround, the story of a robot designed and created by engineers Gregory Powell and Mike Donavan). In Romania, the first forms of robots appeared around the 1980s, but they have been developed since 2018. The doctrine speaks of a new type of criminality "AI Crime" (Thomas C. King, Nikkita Agarwal, Mariarosaria Taddeo, Luciano Floridi,) so AI can be a means or method of committing a crime and from this point of view it must be treated as a subject of law.(Laura Maria Stănilă, „Inteligența Artificială, Dreptul Penal și Sistemul de Justiție Penală. Amintiri din viitor”,

București, Universul Juridic, 2020, p.36) It remains for the future to record whether these are just speculations or will really happen.

Conclusions

AI emerged from the need to improve and implicitly implement the latest generation technologies in suitable fields from industry to medicine and even international security. Digital technology, the algorithms used in the application of AI tools validate the legal personality of both the creator of AI and the user, implicitly their liability in situations where both human and patrimonial damages occur. It is therefore necessary to carry out a critical assessment of the effects that artificial agents produce when they malfunction.

The innovative aspects that AI has brought to forensics, namely the investigation of high-risk crime, as well as the urgent need to access huge volumes of case law and more, have led to performance in terms of professional expertise, by limiting the time of action or by replacing the human being with robots, when they should act in a territory with imminent risk. (the situation of mined lands or critical situations in armed conflicts).

AI can be used for the good of society, but also in harmful actions and for this reason it is necessary to have universal norms that regulate all aspects of the international community.

In the future, AI will be a real support in legal activity through predictive analysis and automatic identification of evidence, analysis of data from a multitude of sources.

The role of AI will, of course, also be one of combating organized crime and facilitating identification processes while maintaining the human factor in the decision-making process.

Whether through the diversity of fields it changes with the passage of time, what remains valid and imperative is the fact that the human being cannot be completely replaced, the act of decision-making being unchangeable regardless of the performance of any AI tool.

The universe will exist as long as humanity exists as well.... Artificial intelligence is the most important innovation of modern man, but it must only be used responsibly as a tool that supports the progress and development of society.

References

1. Laura Maria Stănilă „Inteligența artificială, dreptul penal și sistemul de justiție penală: amintiri din viitor", Editura Universul Juridic, București,2020
2. David McRoney, „Capcanele Inteligenței: învață cum să renunți la gândirea nesănătoasă", Editura Globo, 2019.
3. Lupu, Elena, Coșleț, Ecaterina "Utilizarea inteligenței artificiale în cercetarea științifică: orientări etice" – 2024 - https://rses.ince.md/items/bdb5d9e9-dd66-4f00-974c-ca211ea70de6
4. Russell Stuart, Norvig Peter, „Artificial Intelligence: A Modern Approach," Pearson Education, 2021.