CZU: 343.98+004.8

# REGARDING SOME LEGAL AND ETHICAL ASPECTS CONCERNING THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC ACTIVITIES

Iurie ODAGIU,
PhD, Associate Professor,
Prime rector for studies and quality management,
"Stefan cel Mare" Academy of the Ministry of Internal Affairs,
Republic of Moldova
ORCID: 0000-0002-2474-5299

***Summary***

***The article contains descriptions by way of examples of the legal aspects of applying artificial intelligence algorithms in the detection, investigation, and prevention of crimes. It notes the advanced experience in this field of certain states and the impact on crime investigation processes. It is pointed out that some police structures use artificial intelligence for predicting crime in specific localities or territories. The areas of application of artificial intelligence in maintaining public order and combating crime are mentioned, as well as the legal and ethical aspects of applying artificial intelligence in the process of investigating or preventing crimes.***

***Keywords: artificial intelligence, crime investigation algorithms, crime prevention, information analysis, digitization of criminal investigations, artificial neural networks.***

**Introduction**. Artificial intelligence (AI) is the use of digital technology to create systems capable of performing tasks typically requiring human intelligence [1]. This definition of AI is used by the Council of Europe in the process of drafting and voting on European regulatory acts regarding the application of AI in human activities, economic development, healthcare, transportation development, natural disaster prevention, protection of fundamental human rights, etc. At the international level, the European Union is among the first state organizations to impose regulations on the application and use of artificial intelligence in people's daily lives. As a result, discussions about the utility of AI and the dangers to which humanity could be exposed have divided society into two camps. There are those who support the most advanced implementation of these digital technologies and those who believe that AI presents a dangerous future for humanity, based on its potential to become a threat to security, ethics, and the autonomy of the human species. There are concerns about the possibility of AI being misused in a way that could endanger lives or human rights. There is also a fear that AI could surpass its capacity for control and become too powerful or unpredictable to be kept in check [2].

It is argued that the human species currently dominates other species because the human brain has some distinctive capabilities that other animals do not possess. If AI surpasses humanity in general intelligence and becomes "superintelligent," then it could become difficult or impossible to control by humans. Just as the fate of some animals depends on human goodwill, so too the fate of humanity could depend on the actions of a future superintelligent machine [3]. In the context of the regulations imposed by the European Union regarding the use of AI, it is worth noting that four levels of risk have been identified regarding the use of AI: a minimal or non-existent risk level (e.g., video games, spam filters – areas that will largely not be regulated), a limited risk level (e.g., chatbots – AI systems that pose only limited risks will be subject to very few transparency obligations, such as disclosing that their content was generated by AI, so that users can make in-

formed decisions about further use), a high-risk level (e.g., granting bank loans, managing public transportation, evaluating individuals' performance in various assessments and exams - a wide range of high-risk AI systems will be authorized, albeit subject to a set of requirements and obligations to access the EU market), and an unacceptable risk level (e.g., behavioral-cognitive manipulation, predictive policing activities, emotion recognition in the workplace and educational institutions, as well as social behavior assessment). Remote biometric identification systems, such as facial recognition, will also be prohibited, with some limited exceptions [4]. We observe that from the very beginning, the European legislator limits the possibilities of applying AI in certain areas of police activity.

**Discussions and results obtained**. Regardless of the concerns and risks discussed in society, victims of crimes or offenses, investigative officers, and prosecutors always wish to use advanced scientific tools that lead quickly to the identification of criminals and their whereabouts. In this sense, the emergence and development of artificial intelligence as a useful tool in various social fields have created a very useful premise and opportunity to be applied in the discovery, investigation, and prevention of crimes. Artificial intelligence is traditionally understood as complex computer programs capable not only of acting according to a predetermined algorithm but also of implementing creative functions inherent to humans, such as forecasting, risk assessment, working with incomplete data, etc. In certain spheres of human activity, some artificial intelligence systems are already actively used or beginning to be implemented, for example, in banking, military technologies, advertising, insurance business, medicine, agriculture, etc.

Forensics has always been very receptive to potentially useful technologies for the discovery and investigation of crimes; for this reason, we are very interested in analyzing the perspectives of using artificial intelligence. The renowned artificial intelligence researcher J. Copeland [5, p.7, 8, 15] proposes two approaches to understanding it: bottom-up and top-down. In the first approach, it is about the applied modeling of individual components (processes) of human thinking to solve specific and highly specialized tasks. This approach to understanding artificial intelligence is already actively used in the development and implementation of expert systems, automated databases, etc., in the field of crime detection and investigation. From the perspective of the bottom-up approach to understanding artificial intelligence, the latter involves full-fledged behavior or thinking, namely the complex evaluation of received messages and making balanced decisions based on them in conditions of incomplete and fragmented information.

Analyzing multiple bibliographic sources regarding the application of AI in crime research and law enforcement activities [6; 7], we believe that AI is applied for:

1. Data analysis: Artificial intelligence is used for data analysis and identifying patterns in the information collected during investigations. This can help identify trends and connections between different cases.

2. Facial recognition: AI-based facial recognition systems are used to identify suspects or missing persons in images or video recordings.

3. Analysis of digital fingerprints, firearm traces, and other types of traces: Artificial intelligence can be used for comparing and identifying digital fingerprints, traces on tubes, and bullets in local forensic databases and the framework of forensic information exchange.

4. Creation of information and investigation systems: Police in several states use advanced computer systems to manage and analyze information related to crimes and suspects. These systems can provide support in decision-making and directing investigations.

5. Crime prevention (predictability): By analyzing data and patterns, artificial intelligence can help police anticipate and prevent crimes in certain areas or contexts.

Among the first countries where artificial intelligence has started to be applied in ensuring public security and combating crime, we could exemplify the Netherlands, the USA, the United Kingdom, and others. For example, the Dutch national police have adopted neural networks to as-

sist in case investigations. The system drastically reduces the time spent managing cases. A special automatic algorithm examines case files, helps classify them, and prepares them for investigation. Artificial intelligence reviews documents, analyzes them, examines evidence, and determines the likely level of case complexity. Therefore, neural networks [8] are not able to solve a criminal case on their own, but they do a lot of routine work. According to law enforcement agencies, AI prepares cases in a matter of days, while it may take a police officer several weeks. For example, neural networks are connected to the national DNA database and can therefore uncover common details in seemingly different cases and find missing evidence. As an experiment, artificial intelligence has examined over 1,500 criminal cases across 30 million printed pages. "This type of system does more than just mechanical work; it can see the connection between certain events", emphasizes police officer Roel Wolfert [9] about the utility of neural networks.

In the practice of crime discovery and investigation, automated information search systems are actively used to obtain information on possible investigative directions: the "Block" [10] system, which provides forensic information support for investigating economic crimes; the "Maniac" system, which provides information in the investigation of serial crimes [11, p. 423-430]; the I2 analysis system, which helps establish the contact links of criminals and their interaction with various individuals and institutions [12]; the "Mirror" geographic information system, which operates with spatial data (factual and statistical), and many others [13].

Such digital systems contribute to improving management efficiency by automating activities and the functioning of law enforcement agencies, allowing for a significant reduction in the time costs for decision-making in a specific legal situation, providing enhanced quality and a clearer rationale for the decision made. This becomes possible because any intelligent system is largely the result of the accumulation of all available knowledge in a particular field. In digital systems, human intelligence is used in a concentrated form to solve standard situations in various fields of knowledge, and in these cases, the recommendations issued by the machine are advisory in nature, the decision belonging to the person responsible for the case, although these decisions represent a new, superior level of quality [14].

If we go back in history, digital fingerprints have become a tool for proving guilt or innocence, as well as a means of evidence and identification of individuals in the 19th century [15]. Forensic science did not start with digital fingerprints, but it was the method that captured people's imagination more than any other innovation. Currently, digital fingerprint databases are a norm, but even this is becoming outdated, with the forefront being occupied by genetic profiling, which provides investigative and judicial authorities with more precise methods of personal identification. DNA technology was discovered in 1984 by British geneticist Alec Jeffreys [16]. Analogous to unique digital fingerprints, each person has their own "genetic passport". A reference sample is taken from the person under investigation and compared to the one found at the crime scene. The trace left by a perpetrator is not limited to just a digital fingerprint - a sample can be obtained from blood, saliva, semen, or other suitable liquids or tissues from personal items, such as a toothbrush or a razor, objects touched by the person with hands or lips...). The methodology has already become fully applicable among forensic experts. It is more scientific, meaning more reliable and precise. Within the DNA profile, experts analyze the number of repetitive elements in a selected section of the genome. The accuracy of identification depends on the number of genomic regions analyzed: the more regions, the more precise the results [14]. The polygraph is another technique that "struggles to prove its effectiveness". The latest advancements in polygraph technology include the use of more advanced sensors and data analysis algorithms to improve the accuracy and reliability of polygraph tests. Progress has also been made in developing "non-invasive" technologies that can detect signs of deception without the need for physical sensors on the subject's body. Another significant advancement in polygraph technology is the integration with other technologies. Currently, the results of polygraph activity depend primarily on the expertise

of the examiner conducting the test and the accuracy of the questions asked. The technology itself is partially recognized in some states, not recognized at all in others, and a number of states admit polygraph test results as evidence in legal proceedings. Working with the polygraph will soon undergo fundamental changes. Psychophysiological research through simultaneous detection of changes in breathing, cardiovascular activity, skin resistance, and other physiological parameters will be complemented by the analysis of brain response using electroencephalography (EEG) and magnetic resonance imaging (MRI).

Currently, almost all new cars are equipped with "intelligence": GPS navigation systems, video recording systems, Bluetooth, which allow the driver and passengers to connect their smartphones to the car, etc. The data that users transmit and receive while in the car can be recorded. There is also an internal "computer" responsible for regulating and maintaining temperature and air conditioning, lighting, wipers, cruise control, and more. All of this metadata can be used in forensics. The car will be able to tell us when and where the doors were opened, the trunk, whether seat belts were fastened, if there was an emergency braking or acceleration. All of these can represent valuable forensic information. Officers can use them when investigating traffic accidents, car thefts, the use of vehicles in the commission of crimes, etc. The car can "tell" where and when it traveled, what messages passengers sent and when they called, what websites they visited [17. p. 491].

The most advanced method of using AI in forensic work is predictive analysis. It is believed that a police system is more useful and achieves remarkable success when it prevents crimes, rather than just detecting and investigating them. There is great enthusiasm for using AI in the field of criminal investigation and crime prevention. This enthusiasm is linked to a strong belief that experimenting with new technologies can enhance security as well as improve government efficiency. It is believed that new digital systems lead to rational, scientific, and value-neutral ways of generating knowledge and expertise in the field of criminal justice. Artificial intelligence in this field, therefore, occupies a central position not only in policy documents but can also be observed in numerous examples from practice. The Dutch police are at the forefront of predictive policing practices, at least in Europe, being the first to deploy an AI-based predictive policing system at a national level, and continue to establish an increasing number of predictive policing projects [18].

Artificial Intelligence (AI) plays an increasingly important role in predicting crime, providing tools and technologies that can help authorities anticipate and prevent crimes. Here are a few ways in which AI can be used in this regard:

1. Data Analysis: AI can analyze massive amounts of data, including historical crime data, patterns of criminal behavior, modus operandi, locations where crimes are likely to occur, risk factors, and other relevant information. By using machine learning algorithms, AI can identify patterns and trends associated with criminal activities. Data analysis is a crucial aspect of using AI in crime prediction. Machine learning algorithms enable AI to identify complex correlations and relationships between different variables in the analyzed datasets. For example, AI may discover that certain types of crimes are more likely to be committed in a specific geographic area, during certain time periods, or under certain socio-economic conditions. Additionally, AI can identify risk factors that may contribute to increased criminal activity, such as poverty, lack of education, or high unemployment rates. Through data analysis, AI can generate predictive models that can be used to anticipate future criminal behaviors. These models can guide authorities in preventing crimes or allocating resources efficiently where there is the highest potential for crime occurrence. It is important to note that data analysis conducted by AI is not perfect and there is a risk of generating false or incorrect results, depending on the quality of input data or algorithms used. Therefore, it is crucial that the use of AI in crime prediction be properly supervised and regulated to ensure its accuracy and ethical use.

Therefore, it is crucial that the use of AI in crime prediction be properly supervised and regulated to ensure transparency, ethics, and respect for fundamental human rights. The technol-

ogy company PredPol – short for Predictive Policing – claims that its data analysis algorithms can improve crime detection by 10-50% in some cities. It requires years of historical data, including the type, location, and timing of crimes, and combines this with a wealth of other socio-economic data, which is then analyzed by an algorithm initially designed to forecast aftershocks of earthquakes. The software attempts to predict where and when certain crimes will occur in the next 12 hours, and the algorithm is updated daily as new data emerges. "PredPol was inspired by experiments conducted by the University of California in collaboration with the Los Angeles Police Department", says PredPol co-founder and anthropology professor Jeff Brantingham. This study demonstrated that algorithm-based predictions could forecast twice as much crime and, when used in the field, could prevent twice as many crimes as the best existing practices. The predictions are displayed on a map using color-coded boxes, each representing a 500-square-foot area. Red boxes are classified as "high-risk", and officers are encouraged to spend at least 10% of their time in these territories [19].

2. Early Warning Systems: Relying on data analysis, AI can develop early warning systems that can identify areas or situations with an increased potential for crime. These systems can help authorities take preventive measures to reduce the risk of crimes. By analyzing historical data and identified risk factors, AI can identify patterns and trends that indicate an increased likelihood of crimes occurring in a specific area or under certain conditions. This information can be used to develop predictive models that provide early warnings to authorities about possible imminent criminal incidents. Early warning systems based on artificial intelligence can be extremely valuable for authorities, allowing them to allocate resources efficiently and intervene proactively to prevent crimes. For example, if a predictive model indicates a sudden increase in crimes in a particular area, authorities can intensify police patrols or implement additional security measures to deter criminal activities. It is important to emphasize that these early warning systems are not infallible, and there is a risk of generating false alarms or misinterpreting data. Therefore, it is crucial for authorities to use this information as a complementary tool in decision-making, rather than as the sole source of information.

3. Facial and Pattern Recognition: Facial recognition and pattern recognition technologies can be integrated into surveillance systems to identify suspicious individuals or track their movements. These technologies can be used to identify known criminals or prevent crimes. These technologies use algorithms and machine learning models to analyze facial features or individual patterns and compare them to an existing database or other relevant information. Through facial recognition, surveillance cameras can identify and track individuals based on their unique facial characteristics, such as face shape, eyes, nose, or mouth. This technology can be used to identify suspicious individuals or monitor their presence in a specific location. As for pattern recognition, it refers to the ability of systems to identify and track individual patterns, such as specific movements or behaviors of a person. These patterns can be used to detect suspicious activities or monitor a person's behavior in a particular context. Integrating these technologies into surveillance systems can be useful for authorities in monitoring and preventing crimes, but it also raises certain issues related to privacy, security, and personal data protection. It is important that the use of these technologies be regulated and comply with ethical and legal standards to ensure the protection of rights and to prevent abuses or their inappropriate use.

The Chinese government extensively uses facial recognition in its surveillance systems to monitor and identify individuals in public spaces [20]. Additionally, Chinese companies such as Alibaba and Huawei develop and implement facial recognition technologies for various applications, such as mobile payments and cybersecurity. In the US, government agencies like the Department of Homeland Security and the Department of Justice use facial recognition technologies to identify criminals and ensure national security. Furthermore, companies like Amazon provide facial recognition services to private sector clients [21]. The Russian government utilizes facial rec-

ognition technologies in its security and surveillance systems. Russian companies like NtechLab also develop facial recognition solutions for various industries, such as retail and security [22].

European Union: In the European Union, there are concerns regarding the protection of personal data concerning the use of facial recognition technologies. However, Germany uses these technologies in their security and surveillance systems.

Behavioral Analysis: AI can be used to analyze individuals' behavior and identify behavior patterns that may be associated with criminal activities. Behavioral analysis is a branch of artificial intelligence that focuses on studying and interpreting individuals' behavior to identify specific patterns or trends. This technology uses advanced machine learning algorithms to analyze data related to a person's behavior, such as movements, gestures, speech, or other actions, and to identify signals or cues that may indicate certain types of behavior, including criminal activities. By using AI-based behavioral analysis, systems can learn to recognize and identify behavior patterns associated with criminal activities, such as theft, aggression, or other crimes. These patterns may include changes in a person's movements, reactions to certain stimuli, or other unusual or suspicious behaviors. For example, a surveillance system equipped with behavioral analysis technologies could automatically detect aggressive behavior or shoplifting based on a person's movements or gestures and could alert security personnel or relevant authorities to intervene. The use of behavioral analysis to identify criminal activities poses certain challenges and issues, such as personal data protection, confidentiality, and the potential for errors or discrimination. Therefore, it is crucial for these technologies to be implemented and used in accordance with ethical and legal standards to ensure respect for individual rights and prevent abuses.

**Conclusions.** The development of forensic techniques for the future will take place through the use of AI. The directions of development will focus on advanced behavioral analysis: developing and improving behavioral analysis algorithms to more efficiently identify and interpret behavior patterns associated with criminal activities. This could include the use of facial recognition technologies, natural language processing, voice tone analysis, and other techniques to detect suspicious or unusual behaviors, as well as the use of facial and object recognition technologies to identify and track suspects and vehicles involved in crimes.

Law enforcement, through the use of AI, will develop intelligent monitoring and crime detection systems that will analyze and interpret data in real-time to identify suspicious or illegal activities. These systems could be implemented in public places such as airports, markets, and shopping centers to prevent and quickly intervene in case of crimes.

Law enforcement agencies will increasingly use AI to analyze and interpret large volumes of data to identify patterns and trends in criminal behavior. This could include developing machine learning algorithms to create behavioral profiles of offenders and anticipate possible future criminal actions.

The development of intelligent systems for collaboration and information exchange between law enforcement agencies and other organizations involved in crime prevention and combat, which could facilitate the rapid and efficient exchange of relevant information and data to identify and intervene in criminal activities in a more efficient and coordinated manner (in this regard, INTERPOL, EUROPOL, and other interstate structures for combating transnational crime operate effectively).

**Bibliographical references**

1. https://www.consilium.europa.eu/ro/policies/artificial-intelligence/#what(Visited: 31.03.2024).
2. Bostrom, Nick. Existential risks. Journal of Evolution and Technology. 9 (1): 1–31. (2002).
3. Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies (Ed.: First). https://dorshon.

com/wp-content/uploads/2017/05/superintelligence-paths-dangers-strategies-by-nick-bostrom.pdf. 2014. (Visited: 31.03.2024).
4. Legea privind inteligenţa artificială: PE adoptă un act de referinţă. https://www.europarl.europa.eu/news/ro/press-room/20240308IPR19015/legea-privind-inteligenta-artificiala-pe-adopta-un-act-de-referinta. (Visited: 10.04.2024).
5. Jack Copeland. Artificial Intelligence: A Philosophical Introduction, 1st Edition. Wiley-Blackwell , 1993. P.7, 8, 15.
6. Marc Schuilenburg, Melvin Soudijn. Big data policing: The use of big data and algorithms by the Netherlands Police. Policing: A Journal of Policy and Practice, 2023, 17, 1–9, https://doi.org/10.1093/police/paad.
7. Себякин А. Г. Искусственный интеллект в криминалистике: система поддержки принятия решений. https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sistema-podderzhki-prinyatiya-resheniy.
8. Maša GALIČ, Abhijit DAS, Marc SCHUILENBURG. AI and administration of criminal justice. Report on the Netherlands.
9. https://emerce.nl/event/edaynextgen/sprekers/roel-wolfert/.
10. Bruce Nikkel. Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation, Volume 33, June 2020, https://www.sciencedirect.com/science/article/abs/pii/S2666281720300287.
11. Yasnitsky L., Vauleva S.V., Safonova D., Cherepanov F. The use of artificial intelligence methods in the analysis of serial killers' personal characteristics. Russian journal of criminology. 2015. No.9. P. 423-430.
12. Integrated Law Enforcement: A Holistic Approach to Solving Crime. https://www.redbooks.ibm.com/redpapers/pdfs/redp5116.pdf.
13. https://sparkgeo.com/blog/mirror-world/.
14. Бахтеев Д.В. Искусственный интеллект в криминалистике:состояние и перспективы использования. https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya.
15. Юрген Торвальд. Век криминалистики. Издательство: АСТ, 2020.
16. https://en.wikipedia.org/wiki/Alec_Jeffreys#cite_note-welcome_2004-21.
17. Грицаев С.И., Помазанов В.В., Заболотная Ю.А. Компьютеризация целеопределения и планирования расследования // Научный журнал КубГАУ. 2015. № 108. С. 491.
18. Marc Schuilenburg and Melvin Soudijn 'Big data in het veiligheidsdomein: Onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie' (2021), 20 Tijdschrift voor Veiligheid 4; 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (Amnesty International Netherlands, 2020., Maša GALIČ, Abhijit DAS and Marc Schuilenburg, AI and Administration of Criminal Justice. Report on the Netherlands. https://marcschuilenburg.nl/wp-content/uploads/2023/07/AI-AND-ADMINISTRATION-OF-CRIMINAL-JUSTICE.-REPORT-ON-THE-NETHERLANDS.pdf.
19. Mark Smith. Can we predict when and where a crime will take place? https://www.bbc.com/news/business-46017239.
20. China elaborează reguli pentru utilizarea tehnologiei de recunoaştere facială. https://financial-intelligence.ro/china-elaboreaza-reguli-pentru-utilizarea-tehnologiei-de-recunoastere-faciala/.
21. Public Comment: Face Recognition Technology and Civil Rights, https://www.pogo.org/public-comments/public-comment-face-recognition-technology-and-civil-rights.
22. Leaked documents reveal details on Russia's upcoming surveillance system. https://www.biometricupdate.com/202404/leaked-documents-reveal-details-on-russias-upcoming-surveillance-system.