CONCEPTUAL PRINCIPLES OF USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES DURING INVESTIGATIVE ACTIONS

ZAHUMENNYI Oleksandr - Adjunct of the Department of Organization of Educational and Scientific Training of Kharkiv National University of Internal Affairs, police captain (Kharkiv, Ukraine)

ORCID: https://orcid.org/0000-0002-5580-6285

DOI 10.32782/NP.2023.3.23

The article examines the peculiarities of the use of artificial intelligence technologies during investigative actions. The author analyzes the foreign experience of using artificial intelligence algorithms in criminal proceedings and the possibility of its use in Ukraine. The methodological basis of the research is general scientific and special methods, which are based on the theory of knowledge of legal phenomena, aimed at obtaining complex reliable results. The specificity of the purpose and tasks of the research necessitated the use of the following methods: dialectical, comparative legal, dogmatic, system and structural, modeling, and statistical methods, etc.

It was concluded that today, artificial intelligence is one of the most ambitious directions in the development of information management systems and technologies, which makes it possible to significantly increase the effectiveness of activities in any field, including law enforcement. This circumstance dictates the need for further progressive research into the possibilities of AI, in particular in the field of fighting against crime, as well as consideration of problematic issues of its application, including the ethical nature, legal regulation and responsibility for mistakes made by it.

Keywords: technical means, artificial intelligence, investigative actions, law-enforcement bodies, crime prevention, foreign experience in crime prevention.

Introduction

The rapid development of scientific and technical progress and the wide use of modern information technologies have an undeniable positive impact on social processes. The issue of the use of modern systems and technologies used during investigative actions has been well researched, but the fast development of them requires constant improvement of their implementation in investigative activities. Such prompt response and the introduction of the latest technologies into the criminal process will ensure an effective and comprehensive investigation of criminal cases.

The analysis of scientific researches on this issue gives us grounds to claim that in the science of the criminal process until now there is no common position regarding the understanding of the place and significance of modern technologies used during pre-trial investigation. Scientific literature discusses the problems of using computer, information, digital, communication and other innovative technologies, including forensic technologies, in the practice of crime investigation [1, p.123–129].

Research methodology

The methodological basis of the research is general scientific and special methods, which are based on the theory of knowledge of legal phenomena, aimed at obtaining complex reliable results. The specificity of the purpose and tasks of the research necessitated the use of the following methods: dialectical, comparative legal, dogmatic, system and structural, modeling, and statistical methods, etc.

The dialectical method is used to determine the international experience of using modern artificial intelligence technologies in the paradigm of crime prevention and outline the range of unresolved legal problems related to this. On the basis of the comparative legal and the dogmatic methods the interpretation of legal categories was carried out, the understanding of the concepts of «technical means» and «artificial intelligence» was clarified and deepened. Modeling methods came in handy during the research and substantiation of theoretical models of changes to the Criminal Procedure Code of Ukraine, aimed at improving the legal regulation of the use of information and other modern technologies by employees of operational units when carrying out the tasks of the investigator and inquirer.

Results

One of the achievements of the scientific and technical revolution of the XXI century is the development of artificial intelligence (AI) and robotics, but there is a lack of effective legal regulatory mechanisms in this area. In addition, there is a trend of not so much the impact of law on this shere as the impact of digital technologies on law. Today, the use of modern information systems and AI technologies during investigative actions is quite relevant and ambitious.

Developed countries of the world consider AI as one of the most important strategies for increasing competitiveness and ensuring national security. The achievements of AI are implemented in various spheres of social life, from medicine and educational activities to digital corporations. AI algorithms make it possible to reproduce the mental activity of people with an automated system. At the same time, such systems and the software for their implementation are the subject to teaching according to the principle of the human brain. It means the accumulation of new information against the background of unsuccessful attempts at any action or ineffective decision.

One of the spheres of active implementation of AI is law enforcement. The use of AI in the fight against crime, both at the stage of pretrial investigation and at the stage of prevention and early response to offenses, provides wide opportunities and high potential [2, p.40–59]. Moreover, law enforcement structures increasingly began to move from prevention to prediction of crimes (in the United States of America a corresponding term has already appeared – «predicative policing»).

In this context, the heads of law enforcement structures are trying to develop new strategies and reformat their activities based on this paradigm. The last years one of the key areas of implementation of such strategies in developed countries (USA, China, Europian countries, Japan) is the use of AI and Big Data Technologies. According to experts, the leader of the implementation of AI in the process of fighting against crime is the US Federal Bureau of Investigation. The last decade of the use of AI technologies in the USA is characterized by a rapid transition from the field of theoretical scientific research to the field of concrete practical application. And significant results have been achieved in this field.

Many US cities have implemented data analysis systems that identify trends and predict the likely time and place of crime. Using crime reports, the system identifies areas with the highest likelihood of crime, highlights them on a map, and transmits the information to police officers. This system was developed at the University of California and is known as PredPol. Dozens of police units in Las Vegas, Los Angeles and other cities use this system. PredPol has proven itself positively and now is used outside the United States. Similar systems are used in Germany. The Precobs software also predicts the most likely crime to be committed at a certain place and time.

The use of AI at the stage of pre-trial investigation for the purpose of investigating criminal offenses is actively used when law enforcement agencies already have information about the commission of a criminal offense and the analysis of a large amount of data is required. For example, such tools as NEC Connect are used by the UK police to analyze billions of data collected from financial transactions to identify correlations or patterns of transactions; or the International Child Sexual Exploitation Database (ICSE DB) managed by Interpol, helps to identify victims and/or criminals through the analysis of, for example, furniture and other objects in images of violence or the analysis of background noise in videos. They have proven to be particularly effective in the fight against crime. Thus, with the help of the NEC Connect program, a search with a very high level of complexity and volume of data, which previously required months of research, can now be performed in a matter of minutes and with a high probability of results [3].

Today AI is actively used in law enforcement activities by many leading countries of the world. For example, in the Netherlands, a machine algorithm based on neurotechnology has been used. By studying and analyzing documentation, as well as incriminating circumstances, the neural network helps police officers to significantly save their working time when conducting criminal proceedings.

Police officers in Great Britain also use the achievements of AI in their activities, given the fact that when investigating criminal offenses they very often have to deal with a large amount of information in order to establish the circumstances that are important in the case. Thus, during the investigation of corruption crimes involving Rolls-Royce Holding, the investigators used the capabilities of the detective robot ACE, developed by the London company Ravn, which main task was to identify valuable information for a criminal case. The robot analyzed 600,000 different text files every day. In total, ACE helped 7 investigators process 30 million documents, thereby speeding up the process of investigating a crime [4].

Fujitsu Laboratories Ltd, together with the University of Electrical Communications in Japan, has developed an algorithm for detaining a criminal in urban conditions, which is based on game theory. This theory mathematically describes the technology of defense and attack as a technology of decision-making. Previously, it was difficult to apply in the city due to the increase of the amount of data because of street network growth. The developed «network compression» technology made it possible to cope with this problem. Algorithms are able to direct security resources according to the movement of people and psychological characteristics of the criminal [2, p.55].

One of the most ambitious global projects for the use of AI in law enforcement is the Police Cloud system created by the Ministry of Public Security of the People's Republic of China. This system is designed to integrate different types of information, including data regularly collected by the Chinese police (residential addresses, family relationships, religious affiliations, etc.).

A clear example of the use of analytical and predictive models applied in the PRC is the facial recognition system developed by the Guangzhou company Cloud Walk, which tracks people's actions based on when the suspect went and what he did. The system predicts the most likely crime scene. For example, if someone bought a kitchen knife, he does not yet become a suspect. But if he also buys a hammer and a bag, the suspicion rating for that person increases. This software is used in more than 30 cities and provinces of the country and in real time indicates suspicious persons [5].

The principles and tasks of the development of AI technologies in Ukraine are legally recognized as one of the priority directions in the field of scientific and technological research. Ukraine, as a member of the Special Committee on Artificial Intelligence at the Council of Europe, in October 2019 joined the Recommendations of the Organization for Economic Cooperation and Development on Artificial Intelligence (Recommendation of the Council on Artificial Intelligence, OECD/ LEGAL/ 0449) [6].

AI is becoming the most important factor in the development of the digital economy of any state; however, possible threats from its use raise questions and require legal guarantees for the safe operation of its systems. In addition, the ethical and legal aspects of its use have not been sufficiently studied, it still does not even have a unanimous definition. There is also a problem of forming the conceptual apparatus of «technical means», «technical systems» and «artificial intelligence» as a factor in the regulation of any new sphere.

In order to solve this problematic issue, the decree of the Cabinet of Ministers of Ukraine No. 1556-r, dated December 2, 2020, approved the Concept of the Development of Artificial Intelligence in Ukraine. In this Concept AI is defined as an organized set of information technologies, with the use of which it is possible to perform complex tasks by using systems of scientific methods of research and algorithms for processing information obtained or independently created during work, as well as to create and use own knowledge bases, decision-making models, algorithms for working with information and to determine ways to achieve set tasks [6].

The use of the possibilities of AI in the work of law enforcement agencies, in particular in the direction of conducting investigative actions, is practically in demand and relevant. The capabilities of software in terms of maintaining law and order give a significant advantage to the human potential in the detection, prevention and early response to offenses. Today, Ukrainian law enforcement agencies are actively using artificial technologies in the following areas: facial recognition; use of drones; ensuring road safety; investigation of criminal offenses; prediction and prevention of offenses [7, p.378–380].

In addition, AI is actively used during the creation of automated systems, databases, for the development of algorithms for criminal offenders searching «without delay», identifying potential victims of criminal offenses and in many other areas in the work of law enforcement.

For example, from December 2017 the National Police of Ukraine started the process of implementing a new system for recording all actions related to detained persons — Custody Records. This system was introduced in order to ensure the basic rights of detainees and to prevent baseless accusations against police officers. The information system Custody Records is a part of the information and communication system Information Portal of the National Police of Ukraine and, thus, is a part of the unified system of databases of the Ministry of Internal Affairs of Ukraine. The Custody Records system is being developed at the level of territorial police bodies. In particular, one of its parts — an electronic file with information on all actions regarding a detained person — is regulated at the level of a subordinate regulatory legal act. Further steps should be the normative regulation of the following: 1) the status of the person of the custody officer; 2) infrastructure conditions for the stay of a detained person (zoning of police office); 3) video surveillance systems and work with such data; 4) effective interaction between various officials of law enforcement [8].

Discussion

Regardless of the effectiveness of AI, it should be noted that the results of its work are not always error-free. Undoubtedly, the cases of the assumption of errors by the system are not frequent, but every time they cause a wide public resonance. For example, there was an incident in the USA when the facial recognition system mistakenly «accused» an innocent person, who was wrongly detained by the police and as a result it caused a corresponding reaction from the civil rights union [9, p.106].

In light of this, tech leader Amazon banned police from using its controversial artificial intelligence-based facial recognition software for a year after rights activists raised concerns about the surveillance technology's potential racial prejudice. Amazon said ending law enforcement's use of Rekognition system should give U.S. politicians an opportunity to pass legislation regulating the use of the technology. However, it was pointed out that there were reasons to allow anti-trafficking organizations to continue using it [10].

Similarly, another powerful player in the field of the latest technologies, IBM, represented by the General Director, in its open letter to the US Congress [11] announced the termination of the development of artificial intelligence-based face recognition technology. The company called for «a nationwide dialogue» about whether such technology should be used in law enforcement at all: «IBM strongly opposes and does not condone the use of any technology, including facial recognition technology, for mass surveillance, racial profiling, violations basic human rights and freedoms or any goals that do not correspond to our values and principles of trust and transparency». Frankly speaking, such a decision was not only political, but also business, because the main customer was the US government, and this project did not bring IBM significant income.

The use of the latest technologies and technical means carries a certain danger for both the person and the state. This is caused primarily by the following circumstances:

– vulnerability of technologies on the basis of which critical infrastructures operate (energy supply systems, transport, financial markets, health care, algorithmic justice, border control, military support, etc.);

– carelessly written computer codes for a significant number of programs, the developers of which pay more attention to profitability than to eliminating vulnerabilities;

– the general lack of transparency of the algorithms that govern the world through the specified critical infrastructure, which is explained by the need to preserve commercial, banking, corporate, official or state secrets and is fixed at the level of a regulatory act or a user agreement that no one ever studies;

- the «black box» of AI (due to the full awareness of the algorithm in the principles of its construction and operation, self-learning, self-development, recursive self-improvement, when the first version search for errors within itself, corrects them, forms an improved version of itself and rewrites itself ad infinitum), because the developers themselves can no longer be sure that they understand all the nuances of its work; in the long term. This calls into question the possibility of human control, including due to the lack of a single vulnerable core, when a certain AI algorithm can be dispersed everywhere by blockchain technology, etc.

Thus, there is an eternal confrontation (the state and civil society, the state or society and the criminal, etc.) to which new challenges are added (the confrontation between AI and ordinary intelligence, homo sapiens and digital man (digital human being or homo numeralis, homo digitalis, homo horologium) [12, p.158–170]. This confrontation has a tendency to become a new higher class of people or a new caste, because the results of revolutionary achievements in the fields of bio-, nano-technologies, neurobiology, and genetics will not be available to everyone at once etc).

Conclusion

The introduction of information technologies (and AI technologies are a part of them) is an integral component of the development of socio-economic, scientific and technical, defense, legal and other activities in the spheres of national importance. The lack of conceptual foundations of state policy in the field of AI does not allow creating and developing a competitive environment in the specified spheres of activity.

When studying the foreign experience of using AI algorithms in criminal proceedings, the following directions of its implementation can be distinguished: the use of AI for the purpose of preventing criminal offenses; the use of AI at the stage of pretrial investigation for the purpose of investigating criminal offenses; the use of AI in judicial proceedings.

Today, AI is one of the most ambitious directions in the development of information management systems and technologies, which makes it possible to significantly increase the effectiveness of activities in any field, including law enforcement. This circumstance dictates the need for further progressive research into the possibilities of AI, in particular in the field of fighting against crime, as well as consideration of problematic issues of its application, including the ethical nature, legal regulation and responsibility for mistakes made by it.

With the great potential of using AI technologies, it should be taken into account that AI can not only bring invaluable benefits by increasing and multiplying human abilities, expanding the possibilities for solving a large number of social problems. With all the positivity of its potential for society, AI technologies increasingly act as a criminogenic factor, actively used by offenders, thereby producing an increase in the level of crime and leading to the appearance of new types of it. And this will create a real threat to the interests of citizens, society and the state protected by the criminal law.

References

1. Moiseev O. Technologies in criminology and forensic expertise: correlation and distinction. *Law Journal of Donetsk University.* 2010. No. 2 (24). P. 123–129.

2. Yukhno O. The genesis and problematic issues of the use of the latest technologies and artificial intelligence in forensics, expert activity and pre-trial investigation. *Theory and Practice of Forensic Examination and Criminology*. 2021. Vol. 3 (25). P. 40–59. DOI: 10.32353/khrife.3.2021.04.

3. More than a police records management system. URL: https://www.necsws.com/police-records-management-system/.

4. Nekrasov V. How artificial intelligence progresses: a report on recent achievements. URL: https://www.epravda.com.ua/publications/2019/07/15/649648/.

5. A leading enterprise in the Chinese AI industry. URL: https://www.cloudwalk.com/en/.

6. On the approval of the Concept of the development of artificial intelligence in Ukraine : order of the Cabinet of Ministers of Ukraine dated 02.12.2020 No. 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220.

7. Artemieva K. D. The use of artificial intelligence in the fight against crime // Reforming the legal system in the context of European integration processes: materials of the 6th International Scientific and Practical Conference (Sumy, May 19–20, 2022) / editorial board: prof. A. M. Kulish, Sumy: Sumy State University, 2022. P. 378–380.

8. On the approval of the Instructions for the formation and maintenance of the information subsystem «Custody Records» of the information and communication system «Information Portal of the National Police of Ukraine»: approved by the order of the Ministry of Internal Affairs of Ukraine dated 04.24.2022 No. 311. URL: https://zakon.rada.gov.ua /laws/show/z0629-22#Text.

9. Zahumenna Yu. O. Combating cybercrime in Ukraine as a component of ensuring national security. *European Perspectives: a scientific and practical journal*. 2019. No. 2. P. 106–112. URL: http://ep.unesco-socio.in.ua/wp-content/uploads/2019/10/zhurnal-yevropejski-perspektyvy-2019-2.pdf.

10. Zinchenko P. Amazon banned the police from using its facial recognition system. *Comments UA*. 2002. June 11. URL: https://it.comments.ua/ua/news/technology/amazon-zapretila-policii-ispol-zovatsvoyu-sistemu-raspoznavaniya -lic-654509.html.

11. IBM CEO's Letter to Congress on Racial Justice Reform in IBM Think Policy Blog, June 8, 2020. URL: https://www.ibm.com/blogs/policy/facial-recognitionsunset-racial-justice-reforms/.

12. Radutny O. E. Digital person from the point of view of general and information security: philosophical and criminal law aspect. *Information and Law.* 2018. No. 2 (25). P. 158–171.

Олександр Олександрович
ЗАГУМЕННИЙ,
ад'юнкт відділу
організації освітньо-наукової підготовки
Харківського національного університету
внутрішніх справ, капітан поліції
ORCID: https://orcid.org/0000-0002-5580-6285
e-mail: zagummm@gmail.com

КОНЦЕПТУАЛЬНІ ЗАСАДИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

У статті досліджено особливості використання технологій штучного інтелекту під час проведення слідчих (розшукових) дій. Автор проводить аналіз зарубіжного досвіду використання алгоритмів штучного інтелекту в кримінальному провадженні та можливості його використання в Україні. Методологічною основою дослідження є загальнонаукові та спеціальні методи, які ґрунтуються на теорії пізнання правових явищ, спрямованих на отримання комплексних достовірних результатів. Специфіка мети й завдань дослідження зумовила необхідність використання таких методів: діалектичного, порівняльно-правового, догматичного, системно-структурного, методів моделювання, статистичних методів тощо.

Зроблено висновок, що на сьогоднішній день штучний інтелект є одним із найбільш перспективних напрямів розвитку інформаційних управляючих систем та технологій, що дає змогу значною мірою підвищити ефективність діяльності у будь-якій сфері, зокрема й правоохоронній. Дана обставина обумовлює необхідність подальшого прогресивного дослідження можливостей штучного інтелекту, зокрема у сфері боротьби зі злочинністю, а також розгляду проблемних питань його застосування, у тому числі щодо етичного характеру, правового регулювання та відповідальності за помилки, зроблені з його боку.

Ключові слова: технічні засоби, штучний інтелект, слідчі дії, правоохоронні органи, попередження злочинності, зарубіжний досвід попередження злочинності.