# Artificial intelligence as an object of forensic study: perspectives from a border region

**V V Polyakov[1*], O V Bespechniy[1] and M A Neymark[1]**

[1] Altai State University, 61 Lenina pr., Barnaul 656049 Russia

E-mail: agupolyakov@gmail.com

**Abstract.** From a forensic perspective, the application of artificial intelligence technologies in criminal activity is analyzed. The main directions in the study of this negative phenomenon are determined. Prospects for using machine learning methods in forensics are analyzed. The influence of artificial intelligence in criminal activity and in law enforcement in investigating and preventing crimes on the development of regions is also studied.

**Keywords:** artificial intelligence technologies, criminal activity, crime, investigation of crimes

## 1. Introduction

The economic, social, and migration processes taking place in recent decades have led to the formation of several large, relatively independent territories in the country. They serve as a rallying point both for the neighboring constituent entities of the Russian Federation and the border areas of neighboring states (Central region, Ural, West Siberian, Far Eastern, and others). Such centers are distinguished by well-established economic, logistic, socio-cultural ties, which inevitably affect the level and structure of crime in the region. When committing a number of crimes, criminals are not limited to the territory of individual cities, covering the entire region or its individual parts with their activities, which is especially characteristic, for example, of computer crimes [1], a number of economic crimes [2, 3], organized crime [4], etc.

The active introduction of new technological capabilities (communication, information) into criminal activity, including technologies of artificial intelligence, contributes significantly to these processes. Technologies using artificial intelligence make it possible to commit crimes at a considerable distance from the location of criminals, i.e. within a separate region and also outside the country, while even leaving no digital traces [5, 6]. The use of such methods modifies the criminal activity itself, expanding to a transnational, transboundary character [7].

The modern level of technological progress leads to the emergence of technologies using the principles of artificial intelligence in many areas of our life: manufacturing, banking, transport. There is a growing evidence that the use of artificial intelligence technology in the fight against crime has been begun. This makes it necessary to understand the possibilities of such technologies in terms of forensics and promising areas of their use in criminal proceedings [8, 9].

## 2. Materials and Methods

The study is based on the use of general scientific and special methods: formal-logical, systemic, structurally forensic, etc. For the purposes of the study, the specialized literature is summarized, forensic

investigative practices are analyzed, as well as databases containing information on the methods and consequences of various types of network attacks are studied.

The research novelty is the use of artificial intelligence capabilities in various aspects of improving forensic activities for the investigation and prevention of computer and other high-tech crimes.

## 3. Results

Artificial intelligence technologies are being actively introduced into forensic activities and have broad prospects for their use. The main areas of research and application of artificial intelligence technologies in forensic science are the following: forensic analysis of crimes committed through artificial intelligence technologies; development of technical, tactical, methodical recommendations for the investigation of crimes committed by means of artificial intelligence technologies; development of new methodological approaches to the investigation of crimes; enhancing the capacity of traditional expert research; prevention of these crimes.

## 4. Discussion

Analysis of modern ideas about the use of artificial intelligence technologies in forensic science clearly shows that, as a rule, it is associated with one of the following areas: crime prevention (recognition of signs of impending crime, etc.); capacity building of traditional peer research; algorithmization of the crime investigation process [10]. To a greater extent, the listed directions are based on processing big data using machine learning elements operating within a small number of parameters. Currently, in these areas we are not talking about the use of artificial intelligence in the full sense, since only a small part of the abilities peculiar to the human intellect is used [11]. At the same time, obviously, the subsequent development of technologies will lead to the creation of more sophisticated methods that provide new possibilities of artificial intelligence, similar to the human intelligence.

In our opinion, in the future of forensic science, the following areas related to the use of artificial intelligence technologies should be developed:

1. Expanding the use of artificial intelligence systems in everyday life would lead to the emergence of new types of computer crimes that encroach on the public relations protected by law in these areas. Also, the original application of artificial intelligence will be a new technique used in existing methods of committing a number of traditional types of crimes. We believe that the indicated forms of artificial intelligence are predicted with high probability. In this regard, the task of generalizing the laws and characteristics of criminal activity will be faced by forensic science. These patterns and features are reflected in their respective forensic characteristics, as well as in the identified and described new criminal situations of these crimes [12]. We believe that at the present time, one should very carefully "run into the future," describing specific methods of committing such crimes, as this could provoke potential criminals, becoming for them a kind of "guide to action".
2. The development of general technical and tactical approaches, methods, techniques, and recommendations for the investigation of crimes related to the use of artificial intelligence technology is necessary. The use of artificial intelligence technologies for criminal purposes is largely manifested in specific electronic-digital tracks. This necessitates the development of new technical means for their identification, fixation and removal, and subsequent research, of course. Certain features of the methods and conditions of crimes related to artificial intelligence technologies require their consideration in organizing the whole investigation process and making the development of appropriate tactical and methodical recommendations relevant.
3. Developing a fundamentally new methodology for the investigation of various crimes based on the use of machine learning methods is necessary. Today, this is one of the current trends in forensic science, which has various ways of implementation, primarily we mean the algorithmization of investigation processes. The possibilities of programming the work of investigators have been studied in forensic science for quite some time [13, 14, 15], but it is the use of artificial intelligence technologies that can give such research a new level. The number of

main tasks that can be solved for the implementation of artificial intelligence includes the formation of a sufficient sample for machine learning [16, 17]. In particular, artificial intelligence was obtained as a result of identifying forensic investigative situations developing in the course of investigating crimes and developing algorithms for the operation of machine learning. As a result, based on the technology of artificial intelligence, retrospective and promising versions containing recommendations for the optimal directions of investigation in specific situations of investigation will be created. Artificial intelligence technologies can also be used for partial algorithmization of the entire criminal proceedings (both at the pre-trial and trial stages) [18].

4. The artificial intelligence technologies (neural networks in particular), which allow processing large amounts of information based on heuristic analysis, open up broad prospects for their use in expert activities (pattern recognition: symbols, sounds, images, etc., as well as solving other problems) [19]. The ability of neural networks to learn on the basis of newly obtained information reduces the likelihood of errors during forensic examinations.
5. Artificial intelligence technologies have significant potential in the field of crime prevention. Positive experience of their use in a number of foreign countries (Great Britain, Japan, etc.) indicates this. Domestic forensic science should study and apply international experience. Programs developed on the basis of the neural network can identify the signs of an impending crime, as well as recognize persons whose behavior has a criminal focus. For these purposes, the application of research technology honeypot possible. This technology is a special computer program; it is installed on a separate server or virtual system (website, social network user page, etc.). A relatively easy and unauthorized access is deliberately granted to them for potential criminals through pre-prepared vulnerabilities [20, 21]. Their unauthorized intrusion into an object and further actions are captured in detail by system components, and this allows the honeypot operators to provide control over the actions of the attacker. We believe that the improvement of honeypot technology through using machine learning methods will significantly expand the capabilities of this system in preventing crime in the field of information technology [22].

## 5. Conclusion

We believe that the promising areas of development of artificial intelligence fully fit into the methodology of criminology, carrying for it the great potential of new opportunities. At present, there are all the necessary prerequisites for laying the foundations for the realization of this potential, and at a rather high rate. This will allow to move to a qualitatively new level of detection, disclosure, investigation, and prevention of crimes, especially those that use information technology. In turn, this could affect the development of regions in which anti-crime actors would actively apply systems that use the capabilities of artificial intelligence.

## References

[1] Gavlo V K, and Polyakov V V 2007 *Forensic characteristics of computer information crimes* In Materials of the All-Russian scientific-practical conference: *Law and the State: Priorities of the XXI century* (pp 503-507) (Barnaul, Russia)
[2] Gavrilin Yu V 2009 *Investigation of crimes infringing on information security in the economic sphere: theoretical, organizational-tactical and methodological foundations* (Dissertation of the Doctor of Law) (Moscow, Russia)
[3] Minenko A I 2001 *Problem issues of investigating crimes committed by organized criminal groups in the banking sector* (Dissertation of the Candidate of Jurisprudence) (Krasnodar, Russia)
[4] Nurbekov I M 2010 *Tactical and organizational peculiarities of interaction in the investigation of crimes of an international character* (Dissertation of the Candidate of Legal Sciences) (Moscow, Russia)
[5] Lytkin N N 2007 *The use of computer-technical traces in the investigation of crimes against property* (Dissertation of the Candidate of Legal Sciences) (Moscow, Russia)
[6] Polyakov V V, and Kucheryavsky S V 2006 Study of virtual traces of crimes related to unauthorized access to computer information *Polzunovsky Almanac* **4** pp 55-58
[7] Davydov V O 2018 *Investigation methodology for a transnational criminal activity of an extremist nature*

(Abstract of the Dissertation of the Doctor of Jurisprudence) (Rostov-on-Don, Russia)
[8] Bertovskiy L V 2018 Digital judicial proceedings: problems of the formation of the problem of applying the criminal and criminal procedure legislation In *Collection of materials of the international scientific-practical conference: Problems of Application of Criminal and Criminal Procedure Legislation* (pp 173-178) (Simferopol, Russia)
[9] Zuev S V 2018 The digital environment of criminal justice: problems and prospects *Siberian Legal Vestnik* **4** pp 118-123
[10] Bakhteev DV 2018 Artificial intelligence in forensic science: state and prospects for its use *Criminal Procedure and Criminalistics* **2** pp 43-49
[11] Rubinstein S L 1973 *Problems of general psychology* (Moscow, Russia: Pedagogy)
[12] Polyakov V V 2010 Investigative situations in cases of unlawful remote access to computer information *Reports of Tomsk State University of Control Systems and Radioelectronics* **1**(21) pp 46-50
[13] Vidonov L G 1978 *Forensic characteristics of murders and the system of model versions about persons who committed murder without witnesses* (Gorky, USSR)
[14] Gustov G A 1993 *The program-targeted method for organizing the disclosure of murders* (St. Petersburg, Russia: Institute for Advanced Studies of Prosecution and Investigation Officers of the Prosecutor's Office of the Russian Federation)
[15] Luzgin I M 1981 *Modeling in the investigation of crimes* (Moscow, Russia: Legal literature)
[16] Rozyhodzhaeva G A, and Rozyhodzhaeva D A 2017 Features of the formation of a training sample and the training of a neural network with incomplete input data when solving private medical problems *Scientific Review. Biological Sciences* **5** pp 28-32
[17] Kaftannikov I L, and Parasich A V 2016 Problems of formation of a training sample in machine learning tasks *Vestnik of the South Ural State University. Series: Computer Technology, Management, Radio Electronics* **16**(3) pp 15-24
[18] Vlasova S V 2018 On the issue of adapting the criminal procedure mechanism to the digital reality *Forensic Library: Scientific Journal* **1** pp 9-18
[19] Yeremenko Yu I, and Shatalov A A 2013 Immune algorithm of multiclonal selection in solving problems of handwriting identification *Scientific Statements* **22** pp 218-224
[20] Craig V 2011 Honeypot technologies and their applicability as a strategic internal countermeasure *International Journal of Information and Computer Security* **1**(4) pp 430-436
[21] Chuvakin A 2003 Honeynets: High value security data: An analysis of real attacks launched at a honeypot *Network Security* **8** pp 11-15
[22] Polyakov V V 2017 The honeypot system as an information gathering tool for countering cybercrime *Forensic Library: Scientific Journal* **1**(30) pp 250-254