https://doi.org/10.17816/RJLS50014

Artificial Intelligence in the Fight Against Extremism

Bychkov Vasily,
Candidate of Law Science,
Associate Professor,
Dean of the Faculty of Excellence
of the Moscow Academy
of the Investigative Committee
of the Russian Federation
E-mail: bychkov_vasilij@bk.ru

Prorvich Vladimir,
Doctor of Law Science,
Doctor of Technical Science, Professor,
Professor of the Department
of Criminal Procedure
of the Moscow Academy
of the Investigative Committee
of the Russian Federation
E-mail: kse60@mail.ru

Abstract. *The article reveals the basic regulatory framework for the use of artificial intelligence in Russia. The possibility of using artificial intelligence to fight crime is being analyzed. The need for artificial intelligence to create computer forensic in countering extremist crimes is in development.*

Keywords: *Extremism, extremist crimes, countering, identify, investigation, warning, artificial intelligence, computer forensics.*

Currently, the term “artificial intelligence” (AI) does not cause confusion to anyone. Everyone has become accustomed to the possibility of merging the “machine” and the human mind. This concept has thoroughly transitioned from fiction and entered our everyday reality. In his Address to the Federal Assembly on 15.01.2020, Vladimir Putin, president of the Russian Federation, noted, “Today, the speed of technological changes in the world is increasing many times, and we must create our own technologies and standards in the areas that determine the future. We are primarily talking about artificial intelligence, genetics, new materials, energy sources, and digital technologies.”[1]

To date, a domestic regulatory framework has already been created, which is based on the use of AI in various public relations’ spheres. Russia is among the countries that have strategic planning documents in the field of AI [1, p. 171-185; 2, p. 69-89; 3, p.7-18]. In particular, AI is one of the prior directions in the Strategy of Scientific and Technological Development of the Russian Federation[2]. In the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030[3], AI is named among the main directions of development of Russian information and communication technologies. GOST R 43.0.8-2017 introduced “Information support of equipment and operator activities. Artificially-intellectualized human-informational interaction. General provisions,”[4] approved by the Order of the Federal Agency for Technical Regulation and Metrology of 27.07.2017 No. 757-st.

[1] Presidential Address to the Federal Assembly. URL: http://kremlin.ru/events/president/news (accessed: 12.11.2020).

[2] Approved by the Decree of the President of the Russian Federation from 01.12.2016 No. 642 "On the Strategy of scientific and technological development of the Russian Federation" // Collection of Legislation of the Russian Federation. 2016. No. 49. Art. 6887.

[3] Approved by the Decree of the President of the Russian Federation from 09.05.2017 No. 203 "On the Strategy for the development of the Information Society in the Russian Federation for 2017-2030". 2017. No. 20. Art. 2901.

[4] Electronic fund of legal, regulatory and technical documentation. URL: http://docs.cntd.ru/document/1200146327 (accessed: 12.11.2020).

The National Strategy for the Development of Artificial Intelligence for the period up to 2030 (hereinafter referred to as the Strategy for the Development of Artificial Intelligence) defines the goals and main objectives of AI development in the Russian Federation, as well as measures aimed at its use to ensure the national interest and implement strategic national priorities[5].

Beginning in July 1, 2020, an experiment is planned for the next five years to establish a special regulation to create the necessary conditions for the development and implementation of AI technologies in the Russian Federation, the federal city of Moscow, and the subsequent possible use of the results of AI application[6].

A concept was established for the development of regulation in the field of AI and robotics technologies until 2024[7]. The aims of this concept are to determine the main approaches to the transformation of the regulatory system in the Russian Federation and to provide opportunities for the creation and application of modern information technologies in various sectors of the economy with respect for the citizens' rights and ensuring the security of the individual, society, and the state; to form the foundations of legal regulation for new public relations, emerging in connection with the development and application of AI and robotics technologies and systems based on them; and to identify legal barriers that prevent the development and application of these systems.

According to the Strategy for the Development of Artificial Intelligence, AI is a set of technological solutions that allow human cognitive functions (including self-learning and finding solutions without a preset algorithm) to be simulated and obtain results comparable to the results of human intellectual activity when performing specific tasks.

Complex technological solutions include information and communication infrastructure, software (including those that use machine learning methods), processes, and services for data processing and solution search. According to experts, developments in the field of AI are conducted in two directions: neurocybernetic and logical. The first one is engaged in the creation of universal intelligence, in fact, an analog of the human brain, capable of solving any intellectual problems without human participation, and the second one is aimed at creating applied AI aimed at solving one or more applied problems [4, p. 2].

Currently, the existing regulatory framework and the bulk of scientific research on AI are aimed at improving the efficiency of the economy [5; 6, pp. 201-207] and improving the social sphere.

The Strategy for the Development of Artificial Intelligence states that the use of AI technologies in economic sectors has a general (cross-cutting) nature and contributes to the creation of conditions for improving efficiency and the formation of fundamentally new areas in the activity of economic entities, including through:

- improving the efficiency of planning, forecasting, and management decision-making processes (including predicting equipment failures and preventive maintenance, optimizing supply planning, production processes, and financial decision-making);
- automation of routine (repetitive) production operations;
- use of autonomous intelligent equipment and robotic systems, intelligent logistics management systems;
- improving the safety of employees when performing business processes (including forecasting risks and adverse events, reducing the level of direct human participation in processes associated with an increased risk to their life and health);
- increasing customer loyalty and satisfaction (including sending personalized offers and recommendations that contain essential information);
- optimizing personnel selection and training processes, and creating an optimal work schedule for employees, taking into account various factors.
- using AI technologies in the social sphere, which contributes to the creation of conditions for raising the living standards of the population, including by:

improving the quality of health care services (including preventive examinations, diagnosis, based on image analysis, forecasting the occurrence and development of diseases, and optimal dosages of drugs, reducing the threat of pandemics, automation, and precision of surgical interventions);

improving the quality of education services (including adapting the educational process to students' needs and the needs of the labor market, system analysis of learning performance indicators to optimize professional orientation and early

[5] Approved by the Decree of the President of the Russian Federation from 10.10.2019 No. 490 "On the development of artificial intelligence in the Russian Federation". 2019. No. 41. Art. 5700.

[6] Federal Law No. 123-FZ of 24.04.2020 "On Conducting an experiment to establish a special regulation in order to create the necessary conditions for the development and implementation of Artificial Intelligence technologies in the Subject of the Russian Federation, the Federal City of Moscow and Making Amendments to Articles 6 and 10 of the Federal Law "On Personal Data "" //Collection of legislation of RF. 2020. No. 17. Art. 2701.

[7] Approved by the Decree of the Government of the Russian Federation from 19.08.2020 No. 2129-r // Official Internet portal of legal information. URL: http://www.pravo.gov.ru (date of request: 12.11.2020).

identification of children with outstanding abilities, automation of knowledge quality assessment, and analysis of information about learning outcomes);

improving the quality of the provision of state and municipal services, and reducing the cost of their provision.

However, with the help of AI, both ordinary crimes and crimes of an extremist and terrorist orientation can be committed [7, p. 172], such as the following:

- a terrorist act (Article 205 of the Criminal Code of the Russian Federation), such as an explosion, arson, poisoning of a water supply source, or taking people's lives by using robotics;
- vandalism (Article 214 of the Criminal Code of the Russian Federation); the use of UAV[8] for this purpose is easy to imagine, in which the UAV carries a paint capsule and drops it on a building or structure to desecrate it;
- rendering life-support facilities unusable (Article 215.2 of the Criminal Code of the Russian Federation) by destroying or damaging them by using robots. Committing these actions out of selfish or criminal motives is qualified under Article 215.2 of the Criminal Code of the Russian Federation; in the absence of these motives, these actions qualify under Article 282 of the Criminal Code of the Russian Federation if the goal is to undermine the economic security and defense of the Russian Federation;
- illegal entry into an underground or underwater object protected by the laws of the Russian Federation on departmental or state protection, using robotics, including UAVs (Article 215.4 of the Criminal Code of the Russian Federation);
- theft of nuclear materials or radioactive substances by using robotics to illegally enter a room or storage facility and take possession of the crime subject (Article 221 of the Criminal Code of the Russian Federation);
- illegal acquisition, transfer, sale, theft of weapons, their main parts, ammunition, explosives, explosive devices (Articles 222, 222.1, 226 of the Criminal Code of the Russian Federation), and their illegal movement across the customs border of the Customs Union within the framework of the EurAsEC or the state border of the Russian Federation by the member states of the Customs Union within the framework of the EurAsEC (Article 226.1 of the Criminal Code of the Russian Federation) using robotics, especially UAVs;
- an attack on a sea or river vessel for the purpose of seizing someone else's property, committed with the use of violence or with the threat of its use through the use of robotics, including UAVs (Article 227 of the Criminal Code of the Russian Federation).

The advantages of using AI to commit crimes are obvious.

First, it can be used in dangerous areas, including biologically dangerous ones;

Second, AI ensures the physical safety of the person who uses these technologies to commit a crime because the person is typically far from the place where AI is applied. Thus, the criminal has no fear of being discovered, which psychologically facilitates decision-making related to the violation of socially dangerous acts;

Third, identifying the criminal on the basis of the AI used is difficult.

A detail that should be taken into account is that AI offers certain solutions in accordance with the algorithm that is implemented in a computer program written and debugged by one or more programmers. If a crime is committed via or with the participation of AI, then we are talking about a deliberate form of guilt, because the mechanism or device acts in accordance with the will of the program's creator. This idea implies the indirect commission of a crime [8, p. 2].

From the point of view of criminal law, a necessary step is to distinguish the cases where the relevant persons did not intend to cause any harm to any other persons, legal entities, the state, and society while they were developing an algorithm and creating an AI computer program. At the same time, in some cases, the following unforeseen situations may occur when the results of processing certain information by this version of AI differ significantly from those expected by the corresponding computer program developers:

the algorithm used to write a computer program is designed to compose music based on a selection of certain musical phrases and melodies, their combinations in the original sequence, etc. The use of such a program by its author may lead to the commission of a crime, provided for in Part 1 of Article 146 of the Criminal Code of the Russian Federation or Article 272 of the Criminal Code of the Russian Federation;

AI that involves self-development and independent thinking is created going beyond the original program. At the same time, there is no guarantee that when such an AI commits an act, it will not fall under the crime signs;

AI creates a new AI that commits a socially dangerous act.

Evidently, the processes of developing AI algorithms, creating, and applying appropriate computer programs bring to the fore a number of urgent tasks for their criminal law regulation, which can not only predict the risks of their use, but also provide for liability in the event of harm

[8] An unmanned aerial vehicle (colloquially also UAV or drone) is an aircraft without a crew on board. See: Big Russian Encyclopedia. Moscow; 1994. p. 108.

to the public. A lag exists in the development of criminal law norms in particular because the process of determining the robot's civil status is not complete and the construction of the criminal law risks' concept in AI depends on it.

Experts are invited to work out the issue of criminal liability for illegal trafficking in robotics with AI, which is a gross violation of the rules of robots' operation, resulting in harm to life, human health, or major damage. Such norms will a priori contain blank dispositions. Their adoption will first require the development of appropriate industry legislation that defines the rules for the robotics' turnover that can cause significant harm to public relations, the establishment of a ban, and (or) restrictions in the turnover of certain types of robotics, such as deadly autonomous systems, at least by private individuals. As conditions for the legal turnover of such equipment, the manufacturer must provide for the possibility of robot authentication, maintaining a register of the robots' users or owners [7, p. 178].

To introduce AI into law, experts distinguish the following AI features:

- multitasking;
- ability to work with a large array of information;
- system stability and reliable data storage;
- system flexibility and self-learning ability;
- ability to analyze legal situations with constantly changing conditions [9, p. 215].

AI is already being applied in the judicial system, such as the preparation of procedural documents and working with them. The Casebook program, which is based on machine learning technology, is already operating in judicial practice. With the help of Casebook, the case outcome can be determined (with a certain probability). When filing a claim to the court, the plaintiff can use Casebook to determine the probability that a court decision will be in his favor and, on the basis of this program, develop tactics for his participation in the case.

The introduction of AI programs in office work allows the optimization of work with a large array of incoming and outgoing documents, reduces the complexity of their processing, and thereby expands the judges' ability to study the materials of each case in more depth and improve the quality of the decision's justification.

The European Commission on the Effectiveness of Justice (CEPEJ) in 2018 adopted the Ethical Charter for the Use of Artificial Intelligence in Judicial Systems, which names the priority principles for the use of AI [10, p. 23].

Currently, AI systems are used in operational search operations, investigation, and research of criminal cases, including the use of special knowledge in various forms. Their use by scientists and experts in conducting criminological research is noted. Proposals have also been submitted for their use to counter cyber threats and terrorist threats to the state and society [11, p. 10]. Among such applications are the following:

- formation of a unique system of a criminal's psychological and other characteristics after processing and systematizing available information about him; modeling of his criminal behavior to justify conclusions about the possibility of committing a new crime and even determining its possible time, place, and method;
- analysis of big data obtained from the results of video surveillance in the places where the criminal possibly stays to identify his personality and possible contacts with accomplices;
- formation of visual text materials focused on wanted persons;
- sorting out true and false information about facts and circumstances that are important for establishing the truth in the criminal case under investigation acquired verbally during interrogations of suspects, witnesses, and other persons;
- identification of false information in various types of documents, both on paper and on electronic media;
- tracking and tracing of suspected people's Internet traffic and communications between suspected persons on the Internet and in messengers[9];
- decryption of encoded information, including group processing of criminal case materials, to identify disguised ideal traces of crimes [12, p. 25].

AI is also widely used for processing various statistical data, assisting in document preparation, saturating law enforcement websites with legal information, and making decisions on the criminal acts' qualification [10, p. 25].

Currently, the vast majority of extremist crimes (public calls to carry out extremist activities [Article 280 of the Criminal Code of the Russian Federation], public calls to carry out actions aimed at violating the territorial integrity of the Russian Federation [Article 280.1 of the Criminal Code of the Russian Federation], incitement of hatred or enmity, humiliation of human dignity [Article 282 of the Criminal Code of the Russian Federation), organization of an extremist community [Article 282.1 of the Criminal Code of the Russian Federation], organizing the activities of an extremist

[9] Messenger (real-time messaging system, " ... time, English. Instant...Instant messaging, IM) — instant messaging services (IMS), online consultant programs (OnlineSaler), and client programs (IM), were text messages, audio information, photos and videos can be transmitted and actions such as joint creation of graphic documents can be performed.

organization [Article 282.2 of the Criminal Code of the Russian Federation], financing of extremist activities] Article 282.2 of the Criminal Code of the Russian Federation, Article 282.3 of the Criminal Code of the Russian Federation], and other crimes committed on the grounds of political, ideological, racial, national, or religious hatred or enmity, or on the grounds of hatred or enmity against a social group) are committed using information and telecommunications networks, including the Internet [13-17].

Internet technologies are also used in a number of other crimes aimed at committing suicide:

- incitement to suicide (paragraph "d", Part 2, Article 110 of the Criminal Code of the Russian Federation). For example, in the Tyumen region, Philip Budeikin, the creator of a "death group" in VKontakte, was sentenced for trying to convince two underage girls to commit suicide via the social network. During the investigation, Budeikin's involvement in the deaths of more than 15 teenagers across Russia was checked[10];
- inducement to commit suicide or assistance in committing suicide (paragraph "d", Part 3, Article 110.1 of the Criminal Code of the Russian Federation). Nikita Nearonov, a financial analyst from the Moscow region and the curator of the death group Blue Whale, was sentenced in Chelyabinsk to a real term in a general regime colony. Through an Internet application, he systematically exerted psychological influence on his victims to drive them to suicide, encouraging them to inflict wounds on their bodies and assigning mandatory tasks such as listening to audio and viewing video materials with scenes of violence and suicide, thereby forming a depressive orientation of the victims' consciousness[11]. Moreover, Ganieva F. M. used the social network VKontakte to persuade a minor acquaintance to commit suicide[12];
- organization of activities aimed at inducing suicide (Part 2 of Article 110.2 of the Criminal Code of the Russian Federation). For example, in August 2017, Sh. organized a game on the social network VKontakte to encourage minors inflict bodily harm on themselves, suppressing their psyche and ending the game once they have committing suicide. Sh. involved her brother G. in the plan, and he volunteered to help her find potential participants in the game (called "whales") on VKontakte. Together, Sh. and G. guided the behavior of the teenagers, who had difficult living situations. The court found Sh. guilty of crimes under paragraphs "a, b, v, g", Part 3 of Article 110.1 and Part 2 of Article 110.2 of the Criminal Code of the Russian Federation and paragraph "g", in committing a crime provided by paragraphs "a, g, d", Part 3, Article 110.1 of the Criminal Code of the Russian Federation[13].

Public calls to carry out terrorist activities, public justification of terrorism, or terrorist propaganda are particularly dangerous (Part 2 of Article 205.2 of the Criminal Code of the Russian Federation). While serving his sentence in the Correctional Facility-5 of the Federal Penitentiary Service of Russia in the Orel region, M. used a smartphone with Internet access to post audio files on VKontakte, calling for terrorist activities to be committed and justifying such terrorist acts. In July 2019, the Moscow District Military Court found him guilty of committing a crime under Part 2 of Article 205.2 of the Criminal Code of the Russian Federation[14].

A similar conclusion can be drawn with regard to organizing the activities of a terrorist organization and participating in these activities (Article 205.5 of the Criminal Code of the Russian Federation).

An analysis of published materials on the issues under consideration shows that extremist propaganda is increasingly used by various foreign terrorist organizations. Most often, they use password-protected websites[15] and chat groups with restricted Internet access[16] to recruit new supporters secretly. Internet forums that restrict

[10] Administrator of the "death groups" was sentenced for three years. URL: https://www.gazeta.ru/tech/2017/07/18_a_10793984.shtml (accessed: 12.11.2020).

[11] The court in Chelyabinsk sentenced the curator of the group "Blue Whale". URL: https://www.znak.com/2020-05-27/sud_v_chelyabinske_prigovoril_kuratora_gruppy_siniy_kit_k_realnomu_sroku (accessed: 12.11.2020).

[12] Verdict of the Sudak City Court of the Republic of Crimea dated 07.05.2018 No. 1-25 / 2018 in case No. 1-25/2018. URL: https://sudact.ru/regular/doc/AnhCjvSdlpdj/ (accessed: 12.11.2020).

[13] By the verdict of the Sobinsky City court, the brother and sister were convicted of involving minors in an Internet game of a suicidal orientation. URL: http://oblsud.wld.sudrf.ru/modules.php?name=press_dep&op=1&did=1528 (accessed: 12.11.2020).

[14] Appeal Definition No. 208-APU18-3 / / Review of judicial practice of the Supreme Court of the Russian Federation No. 3 (2018), approved by the Presidium of the Supreme Court of the Russian Federation on 14.11.2018 (ed.from 26.12.2018) // SPS ConsultantPlus.

[15] Website, or site (from the English website: web — "web, network" and site — "place", literally "place, segment, part in the network") is one or more logically connected web pages and is the location of server content. Usually, a site on the Internet is an array of related data that has a unique address and is perceived by users as a whole.

[16] Chat (from the English word "chatter") is a means of exchanging messages over a computer network in real time, as well as software for such communication.

access only to new members of such groups[17] are becoming a source of prohibited information about terrorist organizations and instructions for committing actions of a terrorist nature, including for extremist motives[18]. In February 2021, a 16-year-old and a 17-year-old in Simferopol of the Crimea Republic were detained because they planned to commit terrorist attacks in educational institutions in the Crimea. These teenagers were members of a neo-Nazi Internet community, a member of which was Vladislav Roslyakov, who staged a shooting at the Kerch Polytechnic College in October 2018[19].

Organizing mass riots over the Internet is also socially dangerous (Article 212 of the Criminal Code of the Russian Federation). In July 2019, mass riots took place in Moscow after several candidates for deputies of the Moscow City Duma were not allowed to register because they had the signatures of people who have already died. The candidates did not appeal against the decisions of the election commissions in accordance with the established procedure, instead using the Internet to call on citizens to take part in an illegal rally, "obviously assuming that these actions can provoke mass riots". The participants of the uncoordinated action, who were in the center of Moscow, ignored the legitimate demands of the authorities and grossly violated public order; they used violence against the authorities, broke through the cordon, and paralyzed vehicles' movement on the Garden Ring by going out on the roadway, among other illegal actions[20].

Recently, the problems of detecting and suppressing high-tech crimes related to the rehabilitation of Nazism have become particularly relevant (Article 354.1 of the Criminal Code of the Russian Federation). Thus, the Investigative Committee of the Russian Federation initiated criminal cases against several citizens for posting Nazis' photos on the Internet during the "Immortal Regiment Online" campaign. The Supreme Court of the Russian Federation recognized the verdict for Perm resident Vladimir Luzgin, who was convicted of posting materials on the Internet that approved the activities of Ukrainian nationalist Stepan Bandera[21].

The most obvious use of the Internet for extremist purposes can be observed in real time from the events in the Belarus Republic. The community "Mogilev Partisans" was created on social media, and its members gathered in an abandoned room in the forest near Mogilev, where they practiced street fighting, seizing premises, assault mountaineering, and fighting tactics in the forest[22]. Those who opposed the Belarusian president were located in Poland and Lithuania, and they used Telegram[23] to coordinate the protesters' actions, instruct them to riot, threaten the collapse of the country's tax system and the state currency, and threaten citizens who refused to protest, saying that their private information will be made public[24] and then following through on their threats.

The analysis shows that modern information technologies, including AI elements, have become common tools for extremists. For many crimes of this type, criminals have dangerous tendencies of acquiring law enforcement intelligence in advance. This situation brings to the fore, making the accelerated development of the scientific foundations of computer criminology for extremist crimes related to the use of high-tech tools an extremely urgent issue.

In this regard, one needs to pay attention to the fact that the national program "Digital Economy of the Russian Federation" was adopted[25] in accordance with the Decree of the President of the Russian Federation from May 7, 2018 No. 204 "On national goals and strategic objectives of the development of the Russian Federation for the period up to 2024"[26]. The project's tasks include the creation of a legal regulation system for the digital economy on the basis of a flexible approach to

[17] An Internet forum, or web forum, is an Internet service (platform) for communication between Internet users (more than two participants) on one topic or on several topics (depending on the forum specialization).

[18] Use of the Internet for terrorist purposes. Vienna: United Nations, 2013. URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (accessed: 12.11.2020).

[19] The court has arrested teenagers suspected of preparing a terrorist attack in Kerch. URL: https://www.rbc.ru/rbcfreenews/5e4ec7ca9a7947721f98dc80 (accessed: 12.11.2020).

[20] The court arrested V. Kostenok for participation in mass riots in Moscow on July 27 (addendum). URL: https://www.mskagency.ru/materials/2917207 (accessed: 12.11.2020).

[21] The Supreme Court of the Russian Federation has recognized the legal sentence imposed on a Perm resident for the rehabilitation of Nazism. URL: https://www.kommersant.ru/doc/3078015 (accessed: 12.11.2020).

[22] In Belarus, partisans appeared again. URL: https://eadaily.com/ru/news/2020/09/14/v-belorussii-snova-poyavilis-partizany (accessed: 12.11.2020).

[23] Telegram is a cross-platform messenger that allows messages and media files to be exchanged in many formats. Users can send messages and share photos, stickers, voice messages, files of any type, and make audio and video calls.

[24] Belarus demanded that Poland hand over the founders of the Telegram channel NEKHTA. URL: https://www.rbc.ru/politics/16/11/2020/5fb286059a794701311b1294 (accessed: 12.11.2020).

[25] Approved by the minutes of the meeting of the Presidium at the Presidential Council for Strategic Development and National Projects of 04.06.2019 No. 7 // SPS ConsultantPlus.

[26] Approved by the minutes of the meeting of the Presidium at the Presidential Council for Strategic Development and National Projects of 04.06.2019 No. 7 // SPS ConsultantPlus.

each area, the introduction of civil turnover based on digital technologies, and ensuring information security based on domestic developments in the data transmission, processing, and storage, which guarantees the protection of the interests of individuals, businesses, and the state.

To address these matters and other challenges, a number of federal projects were included in this national project. At the same time, the government of the Russian Federation was instructed to ensure that changes were made to the national program “Digital Economy of the Russian Federation” by December 15, 2019, including the development and approval of the federal project “AI”[27]. In addition, it provides for amendments to the Criminal Code of the Russian Federation related to criminalizing new types of acts committed via modern computer technology and information technology, and ensuring the protection of the rights and legitimate interests of the individual, society, and the state from new threats arising in the transition to a new information society and the knowledge economy. At the same time, attention needs to be paid to the planned creation of non-governmental expert organizations in the field of computer forensics in 2020, a task that was assigned to the Internal Affairs Ministry of Russia and the Justice Ministry of Russia.

In our opinion, the creation of a new criminology area related to the fight against modern high-tech crime cannot focus solely on digital economy protection. The focus on creating an appropriate means of combating crime, including the use of AI, by non-governmental expert organizations under the auspices of the Internal Affairs Ministry of Russia and the Justice Ministry of Russia will not ensure the introduction of a qualitatively new level in the entire system of criminal law protection for protecting the rights and legitimate interests of citizens, organizations, the state, and society as a whole from high-tech crime attacks.

The best scientists and specialists who develop methods and tools for combating high-tech crime problems in all spheres of public life need to be mobilized. We are talking about ensuring security in the transition to a new information society, when atypical tasks constantly arise; thus, the experts’ work should be supported by high-level organizational measures. First, we should pay attention to the scientific potential of state educational institutions that are training highly qualified personnel for law enforcement agencies. The corresponding program of actions formulated in a recently published monograph [18] in relation to the creation of computer criminology for crime detection and investigation in the traditional and digital economy can serve as a basis for the development of such a program in relation to extremist crimes committed with the help of modern information technologies.

The activities conducted within the framework of such a program should aim not only at specific ways of using AI to detect and identify signs of political, ideological, racial, national or religious hatred or enmity, or hatred or enmity against a social group. A significant part of them can also focus on the prompt transfer of data on criminal information users and distributors to specialized law enforcement agencies of data. This approach will avoid the general blocking of messengers[28].

At the same time, a significant part of such activities should focus on creating an integrated scientific foundation for computer criminology to combine the capabilities of all the sciences in the criminal law block (criminal law, criminal procedure law, criminology, operational investigative activities, and forensic expertise) in the fight against modern crime in this area.

References

1. Neznamov A.V. O koncepcii regulirovaniya tekhnologij iskusstvennogo intellekta i robototekhniki v Rossii. *Zakon*. 2020;(1):171-185. (In Russ.).
2. Neznamov A.V., Naumov V.B. Strategiya regulirovaniya robototekh-niki i kiberfizicheskih system. *Zakon*. 2018;(2):69-89. (In Russ.).
3. Ruchkina G.F. Iskusstvennyj intellekt, roboty i ob"ekty roboto-tekhniki: k voprosu o teorii pravovogo regulirovaniya v Rossijskoj Federacii. *Bankovskoe pravo*. 2020;(1):7-18. (In Russ.).
4. Andreev V.K. Dinamika pravovogo regulirovaniya primeneniya iskusstvennogo intellekta. *Journal of Russian Law*. 2020;(3)58-68. (In Russ.).
5. Volynskij A.F., Prorvich V.A. Elektronnoe sudoproizvodstvo po prestupleniyam v sfere ekonomiki (nauchno-prakticheskie aspekty). Moscow: Ekonomika, 2019. (In Russ.). 364 p. (In Russ.).

[27] Approved by the Decree of the President of the Russian Federation from 10.10.2019 No. 490 "On the development of artificial intelligence in the Russian Federation". 2019. No. 41. Art. 5700.

[28] For example, the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor) blocked Telegram in Russia from 16.04.2018 to 18.06.2020, in accordance with two anti-terrorist laws, the so-called Yarovaya’s package: Federal Laws of 06.07.2016 No. 374-FZ “On Amendments to the Federal Law”, “On Countering Terrorism and Certain Legislative Acts of the Russian Federation in Terms of Establishing Additional Measures to Counter Terrorism and Ensure Public Safety”, and No. 375-FZ “On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation in terms of Establishing Additional Measures to Counter terrorism and ensure Public Safety”.

6. Prorvich V.A. Osobennosti kompleksnogo primeneniya special'nyh znanij dlya profilaktiki prestuplenij v sfere tradicionnoj i cifrovoj ekonomiki. *Vestnik ekonomicheskoj bezopasnosti*. 2020;(2):201-207. (In Russ.).
7. Gracheva Yu.V., Aryamov A.A. Robotizaciya i iskusstvennyj intellekt: ugolovno-pravovye riski v sfere obshchestvennoj bezopasnosti. *Aktual'nye problemy rossijskogo prava*. 2020;(6):169-178. (In Russ.).
8. Denisov N.L. Konceptual'nye osnovy formirovaniya mezhdunarodnogo standarta pri ustanovlenii ugolovnoj otvetstvennosti za deyaniya, svyazannye s iskusstvennym intellektom. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yusticiya*. 2019;(4):18-20. (In Russ.).
9. Zakirov R.F. Ispol'zovanie sovremennyh IT-tekhnologij kak sredstvo dostizheniya osnovnyh zadach sudoproizvodstva. *Vestnik grazhdanskogo processa*. 2018;(1):211-219. (In Russ.).
10. Sushina T.E., Sobenin A.A. Perspektivy i riski ispol'zovaniya iskusstvennogo intellekta v ugolovnom sudoproizvodstve. *Rossijskij sledovatel'*. 2020;(6):21-25. (In Russ.).
11. Morhat P.M. Vozmozhnosti, osobennosti i usloviya primeneniya iskusstvennogo intellekta v yuridicheskoj praktike. *Administrator suda*. 2018;(2):8-12.
12. Organizaciya i metodika rassledovaniya otdel'nyh vidov ekonomicheskih prestuplenij: manual. Pod red. A.I. Bastrykina, A.F. Volynskogo, V.A. Prorvicha. Moscow: «Sputnik+», 2016. (In Russ.) 624 p. (In Russ.).
13. Bychkov V.V. Protivodejstvie prestupleniyam ekstremistskoj napravlennosti: kurs lekcij. Moscow: Yurlitinform, 2013. 256 p. (In Russ.).
14. Bychkov V.V. et al. Protivodejstvie prestupleniyam ekstremistskoj i terroristicheskoj napravlennosti: kriminologicheskie, ugolovno-pravovye i kriminalisticheskie aspekty: monografiya. Moscow: Yurlitinform, 2013. 363 p. (In Russ.).
15. Bychkov V.V. Prestupleniya ekstremistskoj napravlennosti: ponyatie, klassifikaciya, obshchie ob"ektivnye i sub"ektivnye priznaki, kvalificirovannye sostavy. *Rassledovanie prestuplenij: problemy i puti ih resheniya*. 2018;4(22):36-41. (In Russ.).
16. Bagmet A.M. et al. Rassledovanie prestuplenij, svyazannyh s ekstremistskoj i terroristicheskoj deyatel'nost'yu: uchebnik. Moscow: YUNITI-DANA, 2019. 719 p. (In Russ.).
17. Bychkov V.V., Rotov V.A. Ponyatie i vidy prestuplenij ekstremistskoj napravlennosti, sovershaemyh s ispol'zovaniem informacionno-telekommunikacionnyh setej. *Rassledovanie prestuplenij: problemy i puti ih resheniya*. 2020;(3):26-31. (In Russ.).
18. Volynskij A.F., Prorvich V.A. Komp'yuternaya kriminalistika v sisteme ugolovno-pravovoj zashchity «tradicionnoj» i cifrovoj ekonomiki. Moscow: Ekonomika, 2020. (In Russ.). 476 p. (In Russ.).

Искусственный интеллект в борьбе с экстремизмом

Бычков Василий Васильевич,
кандидат юридических наук, доцент,
декан факультета повышения квалификации
Московской академии
Следственного комитета
Российской Федерации
E-mail: bychkov_vasilij@bk.ru

Прорвич Владимир Антонович,
доктор юридических наук,
доктор технических наук, профессор,
профессор кафедры уголовного процесса
Московской академии
Следственного комитета
Российской Федерации
E-mail: kse6o@mail.ru

Аннотация. *В статье раскрывается основная нормативная база по применению искусственного интеллекта в России. Анализируется возможность использования искусственного интеллекта в борьбе с преступностью. Формулируется необходимость применения искусственного интеллекта при создании компьютерной криминалистики для повышения эффективности выявления, раскрытия и расследования преступлений экстремистской направленности, совершенных с применением современных информационных технологий.*

Ключевые слова*: экстремизм, преступления экстремистской направленности, противодействие, выявление, раскрытие, расследование, предупреждение, искусственный интеллект, компьютерная криминалистика.*

Список литературы

1. Незнамов А.В. О концепции регулирования технологий искусственного интеллекта и робототехники в России // Закон. 2020. № 1. С. 171–185.
2. Незнамов А.В., Наумов В.Б. Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 69–89.
3. Ручкина Г.Ф. Искусственный интеллект, роботы и объекты робототехники: к вопросу о теории правового регулирования в Российской Федерации // Банковское право. 2020. № 1. С. 7–18.
4. Андреев В.К. Динамика правового регулирования применения искусственного интеллекта // Журнал российского права. 2020. № 3. С. 58–68.
5. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019. 364 с.
6. Прорвич В.А. Особенности комплексного применения специальных знаний для профилактики преступлений в сфере традиционной и цифровой экономики // Вестник экономической безопасности. 2020. № 2. С. 201–207.
7. Грачева Ю.В., Арямов А.А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. № 6. С. 169–178.
8. Денисов Н.Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом // Международное уголовное право и международная юстиция. 2019. № 4. С. 18–20.
9. Закиров Р.Ф. Использование современных IT-технологий как средство достижения основных задач судопроизводства // Вестник гражданского процесса. 2018. № 1. С. 211–219.
10. Сушина Т.Е., Собенин А.А. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве // Российский следователь. 2020. № 6. С. 21–25.
11. Морхат П.М. Возможности, особенности и условия применения искусственного интеллекта в юридической практике // Администратор суда. 2018. № 2. С. 8–12.
12. Организация и методика расследования отдельных видов экономических преступлений: учебно-методическое пособие / Под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: «Спутник+», 2016. 624 с.
13. Бычков В.В. Противодействие преступлениям экстремистской направленности: курс лекций. М.: Юрлитинформ, 2013. 256 с.
14. Бычков В.В. Противодействие преступлениям экстремистской и террористической направленности: криминологические, уголовно-правовые и криминалистические аспекты: монография / В.В. Бычков, Р.А. Сабитов, Т.Р. Сабитов. М.: Юрлитинформ, 2013. 363 с.
15. Бычков В.В. Преступления экстремистской направленности: понятие, классификация, общие объективные и субъективные признаки, квалифицированные составы // Расследование преступлений: проблемы и пути их решения. 2018. № 4(22). С. 36–41.
16. Багмет А.М. Расследование преступлений, связанных с экстремистской и террористической деятельностью: учебник / А.М. Багмет, В.В. Бычков, Ю. М. Зеленков. М.: ЮНИТИ-ДАНА, 2019. 719 с.
17. Бычков В.В., Ротов В.А. Понятие и виды преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. 2020. № 3. С. 26–31.
18. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020. 476 с.