*Advances in Economics, Business and Management Research, volume 81*
1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019)

# *The significance of artificial intelligence and blockchain technologies in criminological and psychological forecasting and prevention of criminal behavior*

Aminov I.I.
Moscow State Law University named after O.E. Kutafin
Moscow, Russia
aminovii@mail.ru

***Abstract* — The article substantiates the expected results of scientific research, which allow to expand the understanding of models, automated algorithms for predicting and preventing criminal behavior on the basis of continuous processing of criminologically relevant information; to develop organizational and legal, psychological and criminological, informational and technological mechanisms for the prevention of crime using artificial intelligence and block-chain technologies. For these purposes, the author considers it necessary to involve various analytical sources, which allow to form profiles of modern criminals in automatic mode, which, in turn, will opportunely allow to identify all kinds of their criminal plans (goals, motives, intentions) and effectively counteract them.**

***Keywords — artificial intelligence, blockchain technology, forecasting, warning, criminal behavior, anti-criminal security, analytics, methodological approach.***

## I. INTRODUCTION

The urgency of using artificial intelligence and block-chain technologies in predicting and preventing criminal behavior is not in doubt since the development of this field of applied informatics is inseparably linked with the Information Security Doctrine of the Russian Federation, approved by Presidential Decree No. 646 of December 5, 2016. In it, as is known, an assessment of the criminological situation in the Russian Federation is given, in connection with the increasing incidences of the use of mechanisms of informational influence on individual and public consciousness by terrorist and extremist organizations in order to force international and social tension, fomenting ethnic and religious

hatred, propaganda of extremist ideology, involvement of new supporters to terrorist activities. The growth of the scale of computer crime in the credit and financial sphere, an increase in the number of violations of the constitutional rights and freedoms of a person and a citizen, including when processing personal data using information technology is emphasized. There is also a steady increase in the scale of computer attacks on critical information infrastructure features, an increase in intelligence activities of foreign states against Russia, as well as an increase in threats of the use of information technologies to damage the sovereignty, territorial integrity, political and social stability of the Russian Federation.

The foregoing suggests that the research of the ability of artificial intelligence and block-chain technologies in predicting and preventing criminal behavior in the conditions of society informatization, inconsistency and fragmentation of legal regulation of relations in the field of information acts as a major scientific problem of great importance for the development of national criminology and law enforcement perfection.

The main array of criminological research by domestic scientists in this field is manifested so far only in the first attempts to translate general theoretical judgments about the need to use artificial intelligence and block-chain technologies into a specific organizational and legal matter — conceptual models for the prevention and prediction of crime. For this purpose, a wide system of knowledge in the field of criminal law, criminology, psychology, informatics, cyber analytics, as well as law enforcement practice is involved. Scientists intend to develop their own position on unsettled or controversial issues, to offer possible solutions to existing organizational, legal and technological problems.

Against a background of the intellectualization of the processes of automated data processing and the immersion of law enforcement agencies into information technologies, the most promising, in our opinion, directions in predicting and preventing criminal behavior that are in line with world developments stand out. Among these directions, the most significant is to use artificial intelligence and block-chain technologies that are able to predict the interests, preferences, desires and even intentions of people in various spheres of life.

An excursus into the history of domestic law enforcement shows that half a century ago, thanks to the development of criminological prediction and prevention, the automatic detection of criminally active persons was carried out, and they were ranked according to the degree of danger of possible crimes on the basis of priority of personality-negative signs. Today, fundamental criminological research is also needed, which makes it possible to put more difficult task to artificial intelligence - how to identify individuals with a certain criminal potential with a forecast of where, when and what crimes should be expected from one or other subjects.

The use of artificial intelligence and block-chain technologies in predicting and preventing criminal behavior, combining the traditional “situational” crime prevention with new opportunities to work with Big Data, should lead to a transition from using single criminological forecasts to creating new predictive criminology, which will significantly

reduce the number of mercenary, violent and other crimes in Russia.

## II. LITERATURE ANALYSIS

Despite the fact, that the works have already been devoted to the study of the problems of information and analytical ensuring of the activities of law enforcement agencies by such authoritative scientists as Yu.M. Antonyan, K.K. Borzunov, V.V. Bychkov, K.K. Goryainov, E.A. Didorenko, E.S. Dubonosov, V.A. Yegorov, S.V. Eskov, S.I. Zakhartsev, A.G. Markushin, V.S. Ovchinsky, S.S. Ovchinsky, N.A. Pogoretsky, B.G. Rozovsky, V.P. Salnikov, G.K. Sinilov, A.N. Hankevich, V.A. Cherkov, A.N. Chistolinov, nevertheless, among the fundamental and applied legal sciences, certain aspects of the information policy and the technical equipment of the units that counteract crime, including in terms of its prevention and forecasting remains without sufficient attention.

Despite the presence of works of foreign authors, such as S.V. Brenner, F. Williams, S. Gordon, D. Denning, W. Zieber, D. Lewis, M. Kabei, B. Colin, D. Marfi, S. Morgan, R. Moore, D. Schinder [1–4], dedicated to artificial intelligence and block-chain technologies in predicting and preventing criminal behavior, most of these works were not translated into Russian and, accordingly, did not receive proper dissemination in the Russian Federation, with the exception of the information that can be obtained from review publications of Russian scientists [5–9]. At the same time, we note that a preliminary analysis of foreign and domestic scientific literature allowed to emphasize the most promising directions in the preventing and predicting criminal behavior.

1. *Active analytics in ensuring anti-criminal security* contributes to erasing the contradictions between the continuous replenishment of resources and occasional (as necessary) resort to them. Active analytics relies on software and hardware systems and is aimed at preventive detection of individuals, who pose certain threats to public order and safety in railway and other transport (detection of train thieves and drug couriers based on automatic verification of operational search databases).

An example of a successful prognostic of active analytics was the initiative research to ensure the safety of the Olympic Games in Sochi (2014). In parallel with the holding competitions and public events in batch mode, data were collected and processed on all persons who attended at sporting events. The signal to the formation of data on persons of operational interest was the fact of purchasing a ticket for a train, plane, or steamer traveling to Sochi.

Active analytics has the greatest prognostic perspectives when carrying out targeted territorial research of a contingent of persons who can be expected with a certain degree of probability to commit a crime (offense) in cities and towns with a high crime situation. Unlike previous years, the task of algorithmization and automation clearly arises here, when processing not only the data already available, for example, for comparison, identification, but also the continuous inflow of new messages.

2. *Prognostic (predictive) analytics in crime prevention* is a qualitatively new direction of law enforcement practice, reflecting the mathematical revolution in data processing. This analytics, generated by the abilities of artificial intelligence (neural networks), enriched by streams of heterogeneous information (secret-service messages, operational reports, background information circulating in the network and social communications), is able to predict criminal motives, goals, intentions in the behavior of citizens. At the same time, at the present stage, it is necessary to carry out fundamental criminological research, which allows to state criminologically significant tasks for artificial intelligence (detecting persons with a certain criminal potential, predicting, which crimes to expect from a particular subject in a space-time relationship).

3. *Relevant analytics in criminological forecasting of conditions, circumstances, place, time, clients and actual doers of crimes.*

The analysis of foreign sources leads to the conclusion that in technologically developed countries there are criminologists-analysts in the police forces, specializing in the research of tactics and strategies of criminal behavior. Based on the analysis of the criminal situation in a particular region, these specialists are able to give the most accurate, capacious and subject forecast - to predict the place, time of the commitment of specific crimes. In their forecasts, they rely on imitating models of the development of a criminal situation, statistical data and patterns of past crimes, expert opinions. Such analytics uses not only the resources of the operational search information, but also criminological models, into which the “live” data of the operational search information is embedded.

Algorithms for processing already existing and incoming information along with a set of existing models allows to detect a possible executor, client of a crime, to focus on their individual personality (temperament features, nature of abilities, value orientations) and behavioral psychological manifestations (goals, motives, intentions, line of conduct ), to clarify the anatomical, functional, attendant signs of appearance and interpret them criminologically correctly.

4. *Global network analytics for detecting security threats.* This direction is actively used by law enforcement agencies of the European Union and the United States. It reflects the technological ideas of collecting and processing data from all available channels of communication, about all recorded events relating to all people and each individual.

## III. RESULTS AND DISCUSSIONS

With global analytics, information on transport tickets, real estate and movable property purchase, banking transactions, electronic payments, phone calls, video-audio fixations, e-mail correspondence is processed in a kind of “melting pot”. The analysis includes information from all federal and municipal authorities (police, prosecutors, fire departments, hospitals and clinics, emergency services, etc.). For biometric identification purposes, this data is accumulated in such powerful specialized systems as Echelon, Carnivore, Einstein, Tempest and others.

Today, information blocks combined into a special chain (block chain) about people and events from the databases of these systems (resource information) along with information from processing centers, transport companies, federal and municipal authorities and services (background information) are sent to special centers where global cyber analytics is carried out [5].

Currently, the Palantir automated research system has gained special popularity, which is able to analyze data streams, detect sequences of heterogeneous and at the same time interconnected events, which made it possible to control and neutralize several terrorist groups.

At the same time, it should be noted that complex research, detecting types and elements of cyber threats, their interrelations, assessment criteria, countermeasures, algorithms for neutralizing actions, etc., as well as developing the organizational and legal basics for the use of digital technologies in predicting and preventing criminal behavior, in our country was not carried out. That is why modern domestic criminologists of different directions and schools are currently focused on developing, first of all, a complex of theoretical, methodological issues of use artificial intelligence and block-based technologies. Without this, it is not possible to actually optimize criminological prediction and the prevention of criminal behavior.

In accordance with this goal, modern criminologists also define research tasks:

- to form an relevant categorical apparatus including the subject of predicting and preventing criminal behavior through artificial intelligence and block-chain technologies;
- to study foreign experience in the application of artificial intelligence and block-chain technologies in predicting and preventing criminal behavior; to prove the appropriateness of its application and adaptation to Russian conditions;
- to state legal content for platform models software designed to predict and prevent criminal behavior;
- to develop models and algorithms for predicting and preventing crime based on continuous processing of criminologically relevant information;
- to establish possible correlations between personal data containing human biometric identification signs (fingerprints, handwriting samples, photo and video images, genomic information, etc.) and criminal behavior, based on the potential of artificial intelligence and block-chain technologies;
- to develop the algorithm and make offers to improve the predictive continuous analysis of background criminologically relevant information, reflecting the characteristics of the individual-personal and moral-psychological manifestations of the person;
- in order to optimize the prevention and prediction of crime, to make offers for consolidating the efforts of all analytical departments of law enforcement agencies to create an unified analytical service;
- together with the teaching staff of leading educational organizations in Russia, for example, the Faculty of Legal Psychology of the Moscow State Psychological and Pedagogical University, to develop a training program for criminologists and analysts who are able not only to find implicit connections and detect invisible patterns in criminal behavior, but also to state tasks appropriate to artificial intelligence [7].

## IV. Conclusions

The results of the theoretical legal and technological development of the problem will create a scientifically-based and practical expedient basis for the concept of the criminal law policy of Russia in the field of ensuring the security of individuals, their rights and freedoms, as well as society and the state from the threats related to crime.

The novelty of such a research can be ensured only in the case of a comprehensive interdisciplinary criminal law, criminological and psychological, information technological approach. Its features should be: 1) statement of new scientific and methodological, scientific and practical tasks; 2) the introduction of new scientific criteria and concepts; 3) the use of innovative and synergistic research methods, in particular for the preventive and predicted activities of the domestic law enforcement system; 4) the development of recommendations and offers to improve the efficiency of countering crimes not only violent, self-serving, mercenary-violent, but also situational; 5) a broad reflection of foreign experience and its adaptation to modern Russian conditions; 6) development of legal content for platform model software in predicting and preventing criminal behavior; 7) study of international experience of cooperation and the development of offers for regulating the order of interaction of states in this field.

It seems necessary to use various information and cybernetic sources to form the profiles of modern criminals in the automatic mode, to detect their various criminal goals, motives, intentions, as well as timely counteract them.

The main methodological approaches of conducting a comprehensive interdisciplinary research devoted to the study of the abilities of artificial intelligence and block-chain technologies in predicting and preventing criminal behavior should be based on the fundamental principles of Russian criminology, methodological principles and requirements of philosophy, sociology, psychology, legal, including criminal legal sciences; reflect the principles of the dialectical interdependence of social processes, phenomena, events in accordance with the specific historical, socio-political, socio-economic and criminological situation.

To conduct a comprehensive interdisciplinary research of the identified problem, it is necessary to use both general (general philosophical, traditional legal) and special methods. It is important to involve methods that found application in concrete sociological (statistical, expert assessments and others), social psychological (observation, inquiry in the form of survey and interviewing, psychological testing, legal statistics, simulation of criminal behavior) research, as well as formative experiment in control groups, modeling of digitalization of criminal behavior, incl. modeling of demand and supply of anti-criminal cyber services.

## *Acknowledgment*

The article is published as part of a scientific project supported by the Russian Foundation for Basic Research (contract number 18-29-16175\18).

## *References*

[1] Brenner, S. (2007) Law in an Era of Smart Technology, Oxford: Oxford University Press; Collin B. The Future of Cyberterrorism / B. Collin // Crime & Justice International Journal. – 1997. – Vol. 13, iss. 2. – P. 51–71;

[2] Jaishankar, K. (Ed.) (2011). Criminology: Exploring Internet Crimes and Criminal Behavior. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group;

[3] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing;
[4] McQuade, S. (ed) (2009) The Encyclopedia of Cybercrime, Westport, CT: Greenwood Press; Tanenbaum A.S. Computer networks / Andrew S. Tanenbaum, David J. Wetherall. — 5th ed. — N.Y. : Prentice Hall, 2011.
[5] Borzunov K.K. Cyberanalysis in securing anti-criminal security // Cyber Security Issues. 2017. No. 2 (20). P. 39–45.
[6] Ovchinsky A.S., Ovchinsky V.S. Operational-investigative analytics in the digital world // Compilation of proceedings of the XXV All-Russian Conference "Informatization and Information Security of Law-Enforcement Agencies". M.: Academy of Management of the MID of Russia, 2016. P. 147–151.
[7] Ovchinsky A.S. Operational-investigative analytics. M.: Publishing house of Shumilova I.I., 2015. - 106 p.
[8] Ovchinsky A.S., Borzunov K.K. Operational-investigative information in the enterprising analytical studies // Economic Security Bulletin, 2016, No. 2. P 180-183;
[9] Foreign experience in the protection of public order with a focus on crime prevention: ARRI MID of Russia. http: // www.ormvd.ru/pubs/102/152018 (access date: 03/21/2019).