The Use of Artificial Intelligence Technologies and Big Data in Law Enforcement

M. A. Yavorsky and S. V. Mikheeva

Abstract The modern world is changing rapidly. The society is already at the stage of its development when information has become an important strategic and managerial resource. Socio-economic transformations and advances in digital science and technology inevitably require radical changes in the organization and management processes of public authorities. The work is dedicated to a topic that is currently relevant, has not been sufficiently studied and requires further research-the use of artificial intelligence (AI) and Big Data technologies in the activities of law enforcement agencies. The article presents some of the main areas of application of automated intelligent processes in investigative, operational and investigative activities, in the field of public order protection and public safety, and in penitentiary institutions. Possible ways to improve the use of AI and Big Data technologies in law enforcement agencies are presented, and tasks aimed at solving "problem areas" of their application are formulated. The work is interdisciplinary in nature, combining the methods and results of previously conducted research in a number of sciences and scientific disciplines.

Keywords AI technologies · Big data · Law enforcement

1 Introduction

AI and Big Data technologies have been one of the fastest growing areas [1, 2]. They are widely used in the public and private sectors: in various sectors of the economy and industry, in transport, in medicine, in the information sphere and other areas of modern society. Modern data analysis tools allow you to solve the problems of finding hidden patterns in the available information; analyze the interests and preferences of people, get data on their health and movements; make a psychological portrait of a

M. A. Yavorsky (✉)
Samara State University of Economics, Samara, Russia

S. V. Mikheeva
Samara Law Institute of the Federal Penitentiary Service of Russia, Samara, Russia

S. I. Ashmarina and V. V. Mantulenko (eds.), *Proceedings of the International Conference Engineering Innovations and Sustainable Development*, Lecture Notes in Civil Engineering 210, https://doi.org/10.1007/978-3-030-90843-0_76

person, determine the traits that unite groups of people; identify “behavioral anomalies” and “hot spots”; establish the financial capabilities of a person, his expenses, transaction data, etc. The list of possibilities of methods for analyzing and systematically extracting large amounts of data is constantly expanding. Among the main areas of application of automated intelligent processes are: information collection, storage and processing of information; analytical and predictive models; implementation of digital investigations; provision of communications and interaction. In the vast majority of countries, law enforcement agencies also use Big Data technologies. These sets of information are also used to uncover and even assess the likelihood of committing crimes, which contributes to their prevention [3, 4]. Using the analysis of information arrays, the social reaction to the committed crimes is determined and predicted, potentially dangerous groups in social networks are identified, etc. [5].

2 Methodology

This research was carried out using both general scientific methods, such as analysis, synthesis, deduction, induction, and specific scientific methods: comparative legal, systemic, and structural. In addition, we effectively used the possibilities of field observation methods and sociological knowledge to obtain the necessary information. The primary sources of the study were scientific publications and reports devoted to the field under study. Along with this, we used the results of a survey of law enforcement officers, students, graduate students and teachers of the legal cycle disciplines of the Institute of Law of the Samara State University of Economics and the Samara Law Institute of the Federal Penitentiary Service of Russia. Information was collected in direct communication with the employees of the investigation and inquiry bodies. The materials obtained are quite representative. This allowed us to consider several important issues related to the use of AI technologies and Big Data in the activities of law enforcement agencies, as well as to formulate proposals and recommendations designed to eliminate “problem areas”.

3 Results and Discussion

In recent years, representatives of various sciences have been paying more and more attention to information technologies: technical, economic, sociological, pedagogical, etc. The analysis of the scientific literature of specialists in the field of economics, technical sciences, sociology, and information security shows a significant interest in the use of digital technologies in various spheres of society. The public is increasingly turning towards understanding the importance of the digital economy, digital transformation and digital development of the state and public spheres. However, the study of the possibilities of using AI and Big Data technologies in legal science and practice, including in the field of law enforcement and public safety, is only gaining momentum. The problematic issues of their application remain insufficiently covered in the literature. Based on the analysis of scientific literature, regulations, law enforcement practice and other sources, the authors analyze the use of automated intelligent processes in investigative, operational and investigative activities, in the field of public order protection and public safety. The tasks and ways of improving the practice of using these technologies were formulated. Digital law enforcement, according to the authors, should become an element of a single model of the social system of the future. To ensure the competitiveness of our society, it is necessary to develop a law enforcement system with advanced management technologies in this area. In the context of information and technological progress, these technologies should become a key factor in optimizing the activities of law enforcement agencies.

The analytical tools and complexes based on AI technology that are being implemented today for law enforcement agencies and special services are capable of:

1. Quickly get (online) access to information, evaluate its qualitative and quantitative parameters. Currently, specialized software systems have been developed and are being used to search for and, most importantly, systematize a huge amount of data from Internet sources in the conditions of "information noise" and information "congestion" (spam, contextual advertising, repeated messages, etc.), which make it difficult to perceive the information you are looking for.
2. Analyze information about committed offenses, including archived data on crime. Thus, existing information systems, analyzing data on offenses, are able to predict the likely time and place of their commission, which contributes to the reduction of crime. The analysis of digital data allows to carry out a controlled criminological experiment, to make decisions aimed at changing the criminogenic situation. Automated analysis of large amounts of data makes it easier to test hypotheses about the causes and conditions of offenses and about the best measures to prevent them in order to develop effective forms and methods of crime prevention.
3. Detect hidden connections between objects and processes (people, cars, mobile phones, places, etc.). Information awareness of law enforcement agencies, generalization and interpretation of data contributes to the establishment of criminal social connections. Software systems are able to identify the active participants of a particular group and the forms of their interaction. Thus, it is possible to identify the opinion of users of social networks on any discussed issue, topic, event, etc. The neural network allows detecting similar offenses, or, for example, serial crimes (multi-episode criminal acts) committed in different regions of the country, to identify patterns and suggest that the investigator combine these cases.
4. To search for and detain criminals. The technology of machine facial recognition in the video stream by full or partial image allows you to identify a person wanted by law enforcement agencies, even in places of mass presence of people (train stations, airports, stadiums, etc.) [6]. Similar technologies were successfully used in Russia at the 2014 Winter Olympics, as well as during the

2018 World Cup [7]. Existing software systems for voice recognition based on comparative analysis with samples that are available to law enforcement agencies, in real time, allow you to identify a person, determine the location of the caller, automatically put the phone on wiretap and record all conversations.

5. Artificial intelligence technologies help to model tactical actions for the detention of offenders, investigative situations of the initial stage of the investigation, contribute to the process of putting forward versions, determining the directions of the investigation of crimes.
6. A separate sector of the development of the use of digital technologies, including AI and Big Data is the penitentiary authorities, which are part of the system of law enforcement agencies in Russia, have their own analytical, technical and operational units. Based on the results of the use of AI, data is collected and processed and decisions are made in various areas of prison activity. AI technology can be used to monitor convicts, ensure security (including using video analytics and predicting the behavior of convicts and prison staff), monitor persons who have been subjected to preventive measures that are not related to detention, and monitor the behavior of released persons. It plans to use automated systems to control the need to create, expand or reduce penitentiary institutions in the regions, depending on the number of persons serving sentences there, and to eliminate the human error factor as much as possible when predicting the behavior of persons in custody or serving sentences (including possible conflict situations). AI technologies can also be successfully applied in the activities of prison psychologists, personnel of logistics, legal and personnel services.

Thus, AI technologies can be applied in many areas of activity of security and law enforcement agencies, penitentiary institutions: investigative, operational-search, organizational and managerial activities, etc. It is difficult to imagine a solution to the problems of ensuring public safety and public order, detection, investigation and prevention of crimes without information technologies. Data sets of operational-search, operational-reference and expert purposes are processed by automated information-reference systems; automated information-search systems; automated expert systems that provide forensic examinations; automated systems for creating portraits; automated fingerprint information systems, etc. In the practice of law enforcement agencies, the possibilities of the Internet for detecting crimes, the scientific organization of their investigation, and the coordination of police activities in general are being introduced. AI technologies and Big Data help optimize traffic for the purpose of safety and fixing traffic violations. They are used to quickly identify criminal events and persons, and to ensure the security of protected objects and information systems of government bodies, institutions and organizations of various forms of ownership. In Russia, the "Safe City" hardware and software complex has been implemented in municipal districts and urban districts, which includes automation systems for the activities of the unified duty and dispatch service, municipal services of various directions, systems for receiving and processing messages, systems for calling emergency and other services of various activities, systems for monitoring, forecasting, alerting and managing all types of risks and threats inherent in this municipality. The “Safe City” complex is a set of functional and technical requirements for hardware and software, regulatory legal acts and regulations of interdepartmental interaction aimed at countering threats to public safety, law and order and the safety of the environment, forming, together with the existing federal security systems, an intelligent multi-level security management system for the subject of the Russian Federation in general and the municipality in particular, through forecasting, response, monitoring and warning of possible threats, as well as monitoring the elimination of the consequences of emergency situations. In the field of law enforcement and crime prevention on the territory of the municipality, the law enforcement unit of the "Safe City" complex allows you to:

- carry out video surveillance and video recording, including the removal, processing and transmission of video streams from video surveillance cameras about offenses and emergency situations, including damage to communications, infrastructure and property;
- analyze video and audio streams, including: automatic event registration based on the video stream analysis system; video event analysis; real-time video stream analysis; face identification and recognition;
- receive and display information about the location of people and moving objects;
- ensure the functions of public control over the activities of representatives of local executive authorities responsible for measures to ensure public order and security.

From a technological point of view, the “Safe City” system is hybrid and has an integrated modular architecture. Within the framework of the complex, various subsystems are operating and being tested: security and fire, engineering (emergency) alarm systems, a system for monitoring access to technical premises, a system for dispatching elevator facilities, a system for turning on and off engineering equipment, a house-wide and individual integrated resource counting system, an emergency dispatcher (voice) communication, a geo-information (topographic) system, and a system for monitoring traffic flows. Thus, the “Safe City” complex is a multi-level intelligent security management system (AI) that can predict, respond, monitor and prevent possible threats, and control the process of eliminating consequences. However, unfortunately, despite the obvious economic and social effects, it is currently not possible to provide all (even large) cities with such complexes in any country in the world, but it is obvious that over time the territorial coverage of such systems will only grow both in Russia and abroad. As some authors rightly point out, the use of AI is the preferred tool in the fight against drug trafficking, illegal migration, cybercrime, illicit trafficking in weapons and radioactive materials, piracy and terrorism [8]. The analysis of investigative and judicial practice and the conducted survey of law enforcement officers shows that information technologies are used in the disclosure and investigation of more than 80% of offenses.

4 Conclusion

The use of digital technologies in the Russian law enforcement system faces a number of problems that significantly reduce the effectiveness of law enforcement agencies. Among the areas of improving the use of AI and Big Data technologies in law enforcement agencies are:

- combining information from disparate sources into a single repository;
- development of software that allows you to identify the necessary information;
- use of software and hardware solutions that accelerate the processing of huge amounts of structured and unstructured information;
- automated documentation of the facts of criminal encroachments on protected (controlled) objects.

The implementation of the possibilities of using AI and Big Data technologies in the activities of law enforcement agencies requires solving a number of tasks:

- the legal regulation of the use of AI technologies and Big Data requires significant changes (especially criminal procedure legislation);
- it is necessary to increase the level of digital competencies of law enforcement officers in the use of AI and Big Data technologies»;
- it is necessary to intensify the development of methodological recommendations on the use of AI and Big Data technologies, to provide them to investigative bodies, inquests, expert units, etc.;
- it is necessary to speed up the equipping of law enforcement agencies with specialized information systems, advanced software and hardware;
- it is necessary to increase the storage time of information transmitted via the internet;
- further development of digital documentation of the facts of criminal encroachments on protected (controlled) objects is necessary;
- it is necessary to continue the deployment of software and hardware satellite navigation devices purchased for the needs of law enforcement agencies;
- it is necessary to develop new methods and secure devices for storing, processing large amounts of data and speeding up information transfer processes.

These "problem areas" and fundamental vulnerabilities in the use of AI and Big Data technologies stand in the way of improving the security system as a whole. Their elimination will allow to integrate the existing records (operational reference, search, forensic, preventive and registration, persons released from places of deprivation of liberty, etc.), will ensure the adoption of adequate management decisions, will significantly increase the level of security and the effectiveness of the disclosure, investigation and prevention of crimes. We believe that the creation of unified centralized operational centers for ensuring public safety will also contribute to the solution of these tasks. In the near future, digital technologies will increasingly penetrate the law enforcement sphere and thus find new applications. The formation of digital competence of law enforcement officers, along with legal, psychological and special training, will become one of the main requirements for police education. AI and Big Data technologies open up huge prospects for fighting crime and improving law enforcement.

References

1. Smith G, Moses L, Chan J (2017) The challenges of doing criminology in the big data era: towards a digital and data-driven approach. Br J Criminol 57(2):259–274
2. Ali A, Qadir J, Rasool R, Sathiaseelan A, Zwitter A, Crowcroft J (2016) Big data for development: applications and techniques. Big Data Anal 1(2)
3. Saheb T, Saheb T (2020) Understanding the development trends of big data technologies: an analysis of patents and the cited scholarly works. J Big Data 7:12
4. Larsen HL, Blanco JM, Pastor Pastor R, Yager RR (eds) (2017) Using open data to detect organized crime threats. Springer, Berlin
5. Williams L, Burnap P (2016) Cyberhate on social media in the aftermath of Woolwich: a case study in computational criminology and big data. Br J Criminol 56(2):211–238
6. Zhou S, Sheng X (2018) 3D face recognition: a survey. HCIS 8(1):1–27
7. Vrankulj A, Artec group 3D facial recognition system deployed at Russia's Sochi airport, https://www.biometricupdate.com/201308/artec-group-3d-facial-recognition-system-deployed-at-russias-sochi-airport, last accessed 2021/03/20
8. Bachmeier L (2018) Countering terrorism: suspects without suspicion and (pre-) suspects under surveillance. In: Sieber U, Mitsilegas V, Mylonopoulos C, Billis E, Knust N (eds) Alternative systems of crime control. Duncker Humboldt, Berlin, pp 171–191