European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.04.02.166

GCPMED 2020
Global Challenges and Prospects of the Modern Economic Development

INFORMATION TECHNOLOGIES IN LAW ENFORCEMENT: OVERVIEW OF IMPLEMENTS AND OPPORTUNITIES

M. A. Yavorsky (a)*, R. Z. Useev (b), S. A. Kurushin (c)
*Corresponding author

(a) Samara State University of Economics, Soviet Army Str., 141, Samara, Russia, yavorm@mail.ru
(b) Samara Law Institute of the Federal Penitentiary Service of Russia, Rylskaya Str., 24 "V", Samara, Russia, useev@rambler.ru
(c) Samara Branch of the State Autonomous Educational Institution of Moscow "Moscow City University", Stara Zagora Str., 76, Samara, Russia, onix.68@mail.ru

Abstract

Currently, many countries, including Russia, have an effective law enforcement system that meets many of the requirements of a modernized society. Every year there is an improvement and development of forms and methods of ensuring law enforcement and public security. Modern society actively uses and implements the results of technological progress in many areas of activity: science, production, art, education, and medicine. Technologies create a new digital reality and digital economy, changing and improving many processes in people's lives. Currently it is not possible to imagine a person without a mobile phone, computer, digital camera or Internet. Digital information technologies are firmly embedded in everyone's life and are an integral part of work or study. However, criminals also use information technology to commit illegal activities, committing qualified crimes remotely. In order to prevent this type of criminal activity, the state needs to improve ways to detect, investigate and prevent information crimes, taking into account the capabilities of information systems. The article discusses some modern information technologies that can or are already applied in the activities of law enforcement. The relevance of using such technologies in law enforcement activities of law enforcement agencies and penitentiary institutions is shown, and examples of their effective application are reduced. Based on the analysis of the capabilities of the considered technologies and tools, it is concluded that they need to be widely implemented and used to solve the problems of combating and preventing offenses.

Keywords: Crime, information technology, law enforcement, penitentiary institutions

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Analysis of scientific literature of specialists in law, information security and information technology shows considerable interest in the problems of digitization in the law enforcement authorities engaged in the fight against crime (Zuev & Nikitin, 2017). The field of offences and the fight against them have undergone major changes, in recent decades criminals are increasingly using technology to their illegal activities (Hutchings et al., 2015). The high degree of introduction of modern information technologies in forensic activities and their development by criminal groups and individual criminals has significantly transformed approaches to the development of criminalistics and its individual areas. Modern forensic support for the process of disclosure, investigation and prevention of crimes is difficult to imagine without special technologies and tools used to study evidence and obtain the necessary information for rapid, complete, comprehensive disclosure and investigation of offenses. Modern technologies also have an impact on the measures taken by the state to prevent offenses (Hummer & Byrne, 2017). And a high level of technical and forensic support for this activity comes to the fore in this issue.

2. Problem Statement

Modern information technologies are developing at a rapid pace, and sometimes what was impossible to imagine a few years ago, today we can see in many areas of human activity, society and the state. The problem of technical armament of law enforcement officers at all stages of the fight against crime has always riveted the attention of scientists and practitioners (Koper et al., 2015). Its relevance is currently due to a factor in the criminal process, criminalistics, operational-search and administrative-jurisdictional activities. In our opinion, one of the areas of effective crime prevention should be the integrated implementation of information technologies in the practice of law enforcement agencies and penitentiary institutions. The necessity of introduction of digital technologies in the sphere of fight against crime caused by several obvious factors:

1. The increase in the number of offences in the commission of which used modern technology (a digital financial instruments, the technology of the blockchain; committing large-scale crimes with the help of information and communication technologies, etc.).

2. The emergence of new delinquent groups (hacker groups, groups preaching violence on the web, etc.).

3. The need to improve measures of criminal law impact and control over crime based on research using digital technologies.

3. Research Questions

In the course of work on this article, the following questions were formulated: What modern information technologies can or are already applied in the activities of law enforcement? How will their application make it possible to qualitatively speed up and improve the processes of disclosing and investigating crimes, their prevention? How is the process of digital transformation of the prison system going (on the example of Russia)? How effective is the use of digital technologies? What is the current challenge facing the law enforcement system and penitentiary bodies in this regard? It is necessary to notice

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

that in the study, we did not set ourselves the goal of a comprehensive research of the stated issues. The study does not claim to be exhaustive and absolute in its conclusions. At the same time, its results allow us to assess the possibilities of digital technologies in such a significant area as state law enforcement.

4. Purpose of the Study

The purpose of research is to consider the issues of using digital technologies in law enforcement in a broad sense. The authors of the article analyzed the possible ways to use information technologies:

- for analytical purposes various types of information in law enforcement (technology of "big data" or BigData);
- in the production of investigative actions, algorithmization of investigative and law enforcement tasks (for example, computer modeling of the scene);
- in the production of handwriting examination (application of artificial intelligence technology);
- in order to search for persons who have committed offenses (use of video surveillance cameras with face recognition technology);
- the use of aircraft (drones) in forensic activities;
- digitalization of the penitentiary system (including in order to increase penitentiary security).

5. Research Methods

The basis of the methodological research is materialistic dialectics as a universal method of cognition. The research is based on a metaphysical approach, dialectical and epistemological concepts. In addition to the main one, private scientific methods are also involved, namely: historical-structural, formal-logical, comparative-legal, modeling, expert assessments, sociological. In addition, sociological research methods were used based on theoretical and empirical methods, supplemented by the concretization of the subject.

Various sources were analyzed to obtain the most accurate information. The information base is represented by open literary sources, expert opinions, normative documents regulating the introduction of digital technologies into the activities of law enforcement agencies both in Russia and abroad. The combination of these methods and techniques allowed us to complete the research task.

6. Findings

Here are just some examples of technologies that need to be integrated into the criminal process, forensics, operational-search and administrative-jurisdictional activities of law enforcement and penitentiary bodies, and which will qualitatively speed up and improve the detection and investigation of crimes, their prevention.

1. Technology "big data" or BigData. This technology opens up new opportunities for analytics of various types of information: audio and video recordings from closed-circuit television camera (CCTV) cameras, data on the traffic of telecom operators' subscribers, information from social networks and forums, text documents. Also technologies of "big data" allow to identify dependencies from different unstructured information databases. The analysis of such data makes it possible to predict the commission of crimes in

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the future, contributes to the advancement of versions, planning the investigation of a criminal case, and the search for suspects and accused who have escaped from the investigation and trial. So, in New York, USA, back in 2007, it was decided to create a centralized public safety operations center. This center analyzes information flows from more than a hundred sources (information from patrol cars, thousands of CCTV cameras, calls from witnesses, etc.). The creation of this system has reduced crime in the city by 27%. One of the big data implementations is a program used by the Chicago police. The program analyzed a database of criminals and was able to identify a list of individuals at risk of murder. Having learned their names, the police conduct preventive work with them, presumably helping to reduce the likelihood of crimes. The program is based on ten main criteria selection. Among them there are a number of figures on the history of bringing a person to the police. The algorithm also takes into account whether a person has been arrested for illegal possession of firearms or for participation in organized crime structures. The algorithm looks for people who meet all or at least some of the selection criteria. Those with the most overlaps on the list of criteria are placed in the highest risk group. According to police, the new algorithm is quite effective. Of the 2.7 million residents of Chicago, the program selected only 1,400 people with an extremely high probability to kill or being killed. More than 70% of the people on this list were shot during 2016. Every 4th shooter was also on the list of the Chicago Police Department. According to law enforcement officials, 117 of the 140 people arrested during the citywide raid against gangs were also on the above list and were at risk (Zhdanov & Ovchinsky, 2020).

2. Technologies of production of investigative actions, algorithms for solving investigative and law enforcement tasks, for example, computer modelling of the scene. The introduction of virtual reality technology into forensic science will allow simulating crime scenes, the simulation is carried out using the laser scanning method. The use of this technology will make it possible to study objects from an arbitrary point, perform measurements and calculations, and automatically generate protocols necessary for the preparation of examination results. As well as in the proceedings in court will allow you to virtually visit the place where the crime was committed, to simulate possible scenarios of actions of individuals at the scene, and a clear and well-reasoned presentation of evidence to the investigating authorities and the court. Going forward, 3D modeling should replace the system of forensic photography and video recording.

In Russia, an IT company has developed virtual training simulators for investigators and mobile applications for inspecting the scene of the incident - “Scene Designer”. The technology allows you to create information layers on terrain maps, draw plans and diagrams of incidents. Each object can be described in detail and provided with audio, photo and video materials from the scene. The technology cuts the time in three times the average investigator spends examining the scene. In the modern world, digital and computer technologies have taken strong positions in almost every area of human activity, and as a result, digital forensics has developed as a specialized branch of forensic science. Digital forensics has the following goals: data discovery, recovery and forensic analysis, as well as collecting evidence using digital technologies. It is worth noting that the area of distribution of digital forensics is quite extensive, it covers not only modern computer technologies, but also their software, electronic data storage, mobile communications, etc. In this regard, when solving crimes, it is necessary to radically change the system of using new technologies (Ovchinsky, 2018).

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. One of the fastest growing areas of technology development is artificial intelligence. These technologies can not only analyze significant amounts of information, but also make some "independent" conclusions based on the results of the analysis. Artificial intelligence is used in various fields: medicine, industry, telecommunications, science, finance, film industry and other areas. Artificial intelligence technology can be successfully applied in handwriting examination. Handwriting examination is carried out, as a rule, by hand by highly qualified experts, therefore the results can be quite subjective and depend on the experience and professionalism of the expert. The use of artificial intelligence allows minimizing the human factor in the examination process. In addition, artificial intelligence analyzes handwriting much faster than an expert and is able to recognize patterns in conditions of strong interference and distortion. Artificial intelligence technologies have an extremely important property - self-learning, which improves the quality of the results obtained. Unfortunately, this technology also has a significant disadvantage: it requires a large amount of initial information for training.

4. Face recognition system. The use of CCTV cameras with face recognition technology allows you to more effectively search for criminals. This system compares faces from the video stream of the CCTV camera with the database of wanted persons. Such a system has been tested in Moscow since 2017, and thanks to it, the police managed to catch more than a hundred criminals.

In 2019, in Russia, the NtechLab company with the Ministry of Internal Affairs of the Russian Federation conducted large-scale testing of recognition systems. Police managed to detain 90 suspects, and thanks to such cameras in the subway, they manage to detain from five to ten wanted people a month. In September 2020, NtechLab announced the testing of a new technology for detecting aggressive actions using cameras (Miller, 2019).

In China, a similar system is also being tested, with one difference: instead of CCTV cameras, police use glasses with a camera. To check a person's identity, a police officer needs to look at him from a short distance and from an angle in which at least seventy percent of the face is visible. The face recognition system will automatically match the received data with the database, while the search takes 2-3 minutes. If there is a match, the system will report the person's name and home address. In the first week and a half of using this technology, seven people were caught at the Zhengzhou railway station, suspected of various crimes (Li, 2018).

5. Unmanned aerial vehicle, or drone. These devices can be used to solve many tasks: to observe large crowds of people, to chase criminals, to look for evidence in places where it is impossible for experts to do this, to inspect buildings where people are dangerous, to catch other drones and quadcopters that break the rules flights, and drones can be equipped with sensors to detect explosives and improvised explosive devices. In Russia, the police began to use drones at the Sochi Olympics in 2014.

The Scientific and Production Association of Special Materials (NPO SM) in the spring of 2019 presented a new drone for the police, equipped with a stun gun and a blinding laser, which causes a short-term loss of vision in a person without negative health consequences (Shmyrova, 2019). The drone is equipped with a camera that allows the operator to assess the situation on the ground and record video. Additionally, a loudspeaker, a siren and a thermal imager can be installed on the drone. In forensic activities, drones can be used to video record a crime scene in hard-to-reach places where the capabilities of an internal affairs officer are limited, such as rocks, roofs, fields, forests, and various bodies of water. The presence of

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

a drone in such situations allows the most objective assessment of the surrounding reality and high-quality filming of the crime scene.

6. Processes of digitalization of penitentiary departments deserve a separate discussion. Currently, Russia is implementing the strategy for the development of the information society in terms of digital transformation of the penitentiary department. The digital transformation of the prison system is a set of organizational and technical measures directed to create a unified information space in its structural units, bodies and institutions, optimizing their activities, as well as organizing interaction with federal executive bodies by introducing digital technologies.

Already today, an integrated security system is used in prisons in Russia, including a control panel for technical security equipment, a loudspeaker communication system, access control and management, operational dispatch communication, CCTV, and alarm systems. All this helps to optimize law enforcement in prisons. The introduced technologies will help to use resources more efficiently, reduce the burden on the staff of correctional institutions, and significantly increase security, which in turn will have a positive effect on their main function - the correction of convicts, the prevention of new crimes by them and other citizens and the restoration of social justice. The digitalization of penitentiary institutions will make it possible to exclude illegal actions of personnel in relation to prisoners, prevent illegal communication of prisoners with the external environment, increase the level of security, fight corruption in prisons, track special vehicles and prisoners, coordinate the production and economic activities of correctional institutions. In addition, digitalization will help increase labor productivity and make the system transparent.

Among others, the goals of digital transformation of the penitentiary system are:

- analysis of the activities of structural units, institutions and for increasing the effectiveness of the implementation of assigned tasks through the introduction of digital technologies;
- creating conditions for readiness for changes in the socio-political and economic situation associated with the transition to the digital economy;
- creation and maintenance of a feedback system with the population, business, expert community, formation and submission of regular public reporting;
- development of free, sustainable and safe interaction of the penitentiary system with citizens, organizations, civil society institutions, government bodies and local self-government;
- organization of information and cyber security, information protection, modelling of information security processes, identification of external and internal sources of threats, means and methods of information protection, countermeasures against targeted external influences;
- development and implementation of a project approach to the implementation of digital technologies;
- formation of technical architecture of computing systems, creation of infrastructure and basic software, design and creation of data storage systems;
- implementation of standards and methodology for the design and construction of information systems, including those based on cloud technologies;
- embedding data-driven decision-making processes in the organization's work processes. To achieve the above goals, it is envisaged to create a department of information technology and digital

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

transformation in the structure of the Russian penitentiary department. This will make it possible to ensure the full implementation of the entire range of tasks of digital transformation of the Federal Penitentiary Service of Russia. An important role is played Federal State Institution "Research Institute of Information Technologies of Federal Penitentiary Service", within the walls of which scientific developments in the field of information technologies are systematically carried out, the results of which are being introduced into the practical activities of the Federal Penitentiary Service of Russia.

7. Conclusion

The above technologies are, to varying degrees, introduced into the activities of the investigative, operational-search, criminalistic and prison authorities in Russia, and this list is far from complete. The development of modern information technologies makes it possible to qualitatively improve the efficiency of detection, investigation and prevention of crimes, as well as their timely suppression. Accordingly, the law enforcement system and the penitentiary bodies of the Russian Federation face the urgent task of further research and implementation of the results of technical progress in their activities.

In the near future, digital technologies are expected to increase significantly in various aspects of law enforcement, as well as in the penitentiary and judicial systems. National experience in the use of such technologies should be available to the international community. International experience can be a good basis for developing relevant legislative initiatives. This will make it possible to maximize the use of modern technologies as a tool for fighting crime.

Acknowledgments

We would like to thank the wonderful translator, Nelly Seiranovna Yeganyan, for her help in translating the article, as well as foreign sources who were useful to us in our work.

References

Hummer, D., & Byrne, J. (2017). Technology, innovation and twenty-first-century policing. In M. R. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice* (pp. 375-389). Routledge.

Hutchings, A., Smith, R. G., & James, L. (2015). Criminals in the cloud: Crime, security threats, and prevention measures. In R. G. Smith, R. C. C. Cheung, & L. Y. C. Lau (Eds.), *Cybercrime Risks and Responses* (pp. 146-162). Palgrave Macmillan.

Koper, C. S., Lum, C., Willis, J. J., Woods, D. J., & Hibdon, J. (2015). Realizing the potential of technology in policing: A mutli-site study of the social, organizational, and behavioral aspects of policing technologies. https://nij.ojp.gov/library/publications/realizing-potential-technology-policing-multisite-study-social-organizational

Li, Y. (Ed.) (2018). Chinese police increase use of smart tech in arrests. http://www.ecns.cn/2018/02-07/291784.shtml

Miller, L. (Ed.) (2019). The Ministry of Internal Affairs summed up the results of the test work of face recognition systems in Moscow. https://www.vedomosti.ru/technology/articles/-2019/06/26/805163-mvd-podvelo

Ovchinsky, V. S. (2018). *Crime and fighting the basics in the digital world.* IPM named after M. V. Keldysh.

https://doi.org/10.15405/epsbs.2021.04.02.166
Corresponding Author: M. A. Yavorsky
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Shmyrova, V. (Ed.) (2019). A paralyzer drone with an electric shock was created for the Russian police. https://www.cnews.ru/news/top/2019-05-15_dlya_rossijskoj_politsii_razrabotali_strelyayushchego

Zhdanov, Yu., & Ovchinsky, V. (2020). *Cyberpolice of the XXI century. International experience.* International Relations.

Zuev, S. V., & Nikitin, E. V. (2017). Information technologies in solving criminal procedure problems. *Russian Journal of Criminology*, *11*(3), 587-595.