European Proceedings of
Social and Behavioural Sciences
EpSBS

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

DOI: 10.15405/epsbs.2022.01.102

SLCMC 2021
International conference «State and law in the context of modern challenges»

INFORMATION AND COMMUNICATION TECHNOLOGIES IN CRIMES AND CRIME PREVENTION

Alexander N. Varygin (a), Irina A. Yefremova (b), Roman A. Sevostyanov (c)*
*Corresponding author

(a) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, van808@yandex.ru
(b) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, efremova005@yandex.ru
(c) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, postmeister@ yandex.ru

Abstract

The article deals with the criminological analysis of crimes committed with the help of information and communication technologies. At present, such crimes are quite common in Russia and other countries. It is stressed that these criminal attacks have a pronounced trend of growing. For example, from 2017 to 2020 their number increased 5 times, and sometimes law enforcement agencies cannot efficiently combat such crimes. Various approaches to the definition of the term “information and communication technologies” are discussed. Attention is drawn to the fact that information and communication technologies are used by criminals not only in the process of committing crimes encroaching on relations that develop in the sphere of the usual computer information circulation, but also in committing crimes that encroach on other public relations protected by the Russian criminal law. Some measures for crime prevention to be undertaken by law enforcement agencies with the help of information and communication technologies are proposed. It is stated that crimes under discussion provide a criminological picture of modern Russian crime and, above all, that of crime of the nearest future. To prevent such crimes new, non-trivial approaches and counteraction measures are necessary. Such approaches and measures require fundamental research of the above-mentioned criminal encroachments.

Keywords: Crime, technology, crime prevention, information and communication technologies, information and communication technologies

https://doi.org/10.15405/epsbs.2022.01.102
Corresponding Author: Roman A. Sevostyanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Development of the information space creates new opportunities that allow criminals to use various technologies that facilitate the commission of crimes. Society faces not only new, rapidly developing types of crimes. Criminal activity sometimes outstrips the capabilities of law enforcement agencies to prevent it and brings the problem of combatting crime to the global international level. In particular, one should mention cybercrimes, economic crimes, crimes related to illegal human trafficking, slave labour, juvenile delinquency, and so forth.

2. Problem Statement

In the Russian Federation, there is a steady growth of criminal attacks committed with the help of information and telecommunications technologies. According to statistics, law enforcement agencies registered 90,587 such criminal assaults in 2017, 174,674 – in 2018 (an increase of + 92.8 %), 294,409 crimes – in 2019 (+68.5 %), and 510,396 crimes – in 2020 (+73.4 %).

Thus, during the period under consideration the number of criminal acts committed with the help of information and telecommunication technologies increased more than 5 times and their share in the structure of crime is from 4.4 to 25 %, while the detection rate of such crimes is no more than 25 %. Despite the fact that official statistics show an increase in the considered criminal attacks, it still reflects only a small part of them, because crimes committed with information and communication technologies have a high degree of latency.

The current situation indicates that there is a great need for developing effective measures to prevent crimes committed with the help of information and communication technologies. Specialized scientific research on the development of measures for preventing criminal encroachments under consideration is rare in Russia. They also have a rather narrow focus, while prevention of such criminal encroachments requires a comprehensive approach (Broadhurst et al., 2014), which is unthinkable without the development and understanding of the conceptual apparatus.

3. Research Questions

The subject of the study involves the norms of the current Russian legislation, the data of the official statistics, the materials of investigative and judicial practice, criminological features of crimes committed with the help of information and communication technologies and measures for their prevention.

4. Purpose of the Study

The purpose of the study is to analyse information and communication technologies used by criminals and to develop a conceptual framework for crime prevention employing the latest information and communication technologies.

https://doi.org/10.15405/epsbs.2022.01.102
Corresponding Author: Roman A. Sevostyanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

The study is based on the dialectical method of cognition, as well as general research methods (analysis and synthesis, induction and deduction, logical, systemic and structural methods) and private methods of cognition (theoretical and statistical, formal and legal ones).

6. Findings

Currently, the Russian legislators in Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection", which is one of the fundamental legislative acts of the Russian state forming the basis of legal regulation in the field of production, distribution, protection of information, and the use of information technologies in the Russian Federation, define information technologies. However, this definition is reduced only to the processes and methods of performing actions related to information (search, processing, etc.) and to the methods of their implementation.

The community of scholars and law enforcement agencies uses not only the term "information technologies", but also another, more general term that is wider from the semantic point of view – "information and communication technologies". Its meaning includes not only the processes and methods of performing actions related to information ("information technologies"), but also refers to a set of technical, software and hardware equipment, devices and applications that are directly intended for performing actions related to information (search, transfer, etc.) (Khasimova, 2016). This term in our opinion is the most appropriate in the framework of this study allowing a more inclusive consideration of criminal attacks committed with the help of various technical facilities and devices that are currently available and being developed. We will use this term in the paper.

Some scholars suggest that information and communication technologies should be understood not only as software and hardware tools and devices that operate on the basis of computer technology and are designed to perform various operations related to information (collection, processing, use, etc.), but also as methods and processes that form a uniform system (Azimov & Shchukin, 2009).

On the one hand, the term "communication" means transmission of a message through language and other sign systems (Efremova, 2000). Technology, on the other hand, is a set of methods, processes, methods, and techniques that are present and used in a particular branch of production, a particular business (Efremova, 2000; Ozhegov, 1991). Based on this, it should be stated that the content of the term in question includes a set of methods and processes designed to perform operations related to information.

A number of authors prefer the terms "digital technologies", "computer technologies", "new information technologies" rather than the term "information and communication technologies," noting that digital technologies are the most dynamic and rapidly developing technologies in the field of telecommunications and informatization of society (Sukhodolov et al., 2019).

The term "digital technologies" and the term "information and communication technologies" are related as a particular and the general, because the term "information and communication technologies", unlike digital technologies, includes not only them, but also other technologies, whose purpose is to carry out information-related operations. Such an approach is also applicable to the terms "computer technologies" and "new computer technologies".

https://doi.org/10.15405/epsbs.2022.01.102
Corresponding Author: Roman A. Sevostyanov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Information and communication technologies in crime can be interpreted in two ways. On the one hand, they are used by criminals not only for committing crimes that encroach on relations developing in the sphere of the usual computer information circulation, but also for criminal encroachments on other public relations protected by the Russian criminal law (e.g., phishing). On the other hand, they are an effective tool for successful combating and preventing specific crimes (Ovchinsky, 2018).

International cooperation can positively influence the prevention of crimes under study, because the use of various technologies by criminals in their activities, as it has already been noted, is a problem not only of a single country, but also of the world community as a whole. For a long time, criminals have been using information and communication technologies to commit criminal attacks threatening the entire world community. In this connection, there is a need for the world community to develop an international convention on countering the use of information and communication technologies by criminals.

Special criminological measures to prevent criminal encroachments committed with information and communication technologies include: program-targeted planning of activities by law enforcement agencies to prevent criminal encroachments under consideration; setting up of specialized bodies or units, whose activities could be aimed at preventing these crimes; optimization of coordination of the activities of law enforcement agencies and other state bodies in the field of crime prevention; improving the level of knowledge in the field of information and communication technologies of law enforcement officers detecting and investigating criminal encroachments (Spasennikov, 2018a, 2018b), as well as improving the level of technical support for law enforcement agencies in detection and disclosure of criminal encroachments under consideration.

Theoretical and practical aspects of various information and communication technologies usage in prevention of criminal encroachments are also considered by a number of foreign researchers (Aiello, 2018; Hagen, 2016; Hannah–Moffat, 2018; Revier, 2018). More recent studies have been done by Russian scholars (Kravtsov, 2018; Osipenko, 2015; Sukhodolov et al., 2018; Yakovets, 2017), who use the term “digital criminology”. This is a new direction in criminology meeting the needs of information space development. It studies the use of “new”, “digital” technologies by criminals in committing criminal attacks and in their prevention.

The analysis of the existing studies carried out both by foreign and Russian scholars allows us to identify the main directions of crime prevention in general and crimes committed using information and communication technologies in particular.

First, we should mention the use by law enforcement agencies of “big databases” (Big Data) with online access to them, which, undoubtedly, is a positive aspect that allows law enforcement agencies to work using all opportunities of the available database of information online. Big Data is employed for performing operations related to information (its collecting, processing, etc.). This method can be used by law enforcement agencies to process not only a large amount of information, but also information that has a high rate of accumulation. Big Data is actively used by law enforcement agencies of foreign countries for preventing and combatting crime.

Progressive steps in this direction are also being taken in the Russian state. Currently, law enforcement agencies have such databases as Federal Information System of the State Road Safety Inspectorate, Service for Centralized Accounting of Weapons, “Sledopyt-M”, Service for Ensuring the

Protection of Public Order, and so forth. In order to optimize the activities of law enforcement agencies in crime prevention, it seems advisable to create a uniform centralized network that would integrate all the above-mentioned databases, and allow measuring various data on crime that is committed on the territory of the Russian state.

Second, law enforcement agencies should make more active use of computing capabilities, expert systems and artificial intelligence, the latter being a modelling part of the psychophysiological and mental processes of an individual. In particular, in some countries, programs have already been developed and are actively used to predict the commission of crime at a specific place and by a definite person. The use of artificial intelligence is possible when creating various expert programs that provide an algorithm for the actions of investigators and inquirers qualifying the act according to the list of the necessary investigative actions in a particular criminal case. Certain steps in this direction are being made, including those undertaken by scholars of Saratov State Law Academy (Bytko & Mitkin, 2020).

Third, it is necessary to develop technical tools and software that allow identifying individuals and finding fictitious data provided by criminals, for example. These tools are represented, first, by systems allowing comparing a person's face with photos, portraits available in the database and eventually identifying such a person.

Fourth, there is a necessity to use modern technical means for identification of criminals, detection of explosive devices, explosives, and narcotic substances. In this case one should mention the active use in the activities of law enforcement agencies of drones, robots, and other technical facilities and devices allowing the police to detect not only criminals, but even identify some kind of extraordinary criminal situation and intervene in it. For example, such robots are actively used in China.

Fifth, it is necessary to use new technologies to protect citizens, that is, to prevent their victimization in cyberspace. It mainly involves ensuring the information security of the population of the country; developing measures to protect the personal data of people, so that criminals could not use them, and so forth.

7. Conclusion

Within the framework of this article, we have not touched upon all aspects of crimes committed with the help of information and communication technologies, and have presented only the most general measures for preventing such crimes. We believe that the problem of such crimes and their prevention is currently the most important in the country. Such crimes present a picture of modern crime and largely that of the crimes of the future. To prevent them, new, non-trivial approaches and counteraction measures are necessary. They, in turn, require fundamental scholarly research of the criminal encroachments under consideration.

References

Aiello, M. F. (2018). Policing through Social Networking: Testing the Linkage between Digital and Physical Police Practices. *The Police Journal, 1*, 89–101.

Azimov, E. G., & Shchukin, A. N. (2009). *A New Dictionary of Methodological Terms and Concepts (Theory and Practice of Language Teaching).* ICARUS Publishing House.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology, 8*, 1–20.

Bytko, S. Yu., & Mitkin, S. B. (2020). Legal Information System "DRAGON-law" Based on the Algorithmic Visual Language "DRAGON". In N. N. Kovaleva (Ed.), *Problems and Challenges of the Digital Society: Trends in the Development of Legal Regulation of Digital Transformations*, *in 2 volumess.* Vol. 1 (pp. 322–334). Publishing house "Saratov State Law Academy".

Efremova, T. F. (2000). *A New Dictionary of the Russian Language. Explanatory and Educational, in 2 volumes*. Russian language.

Hagen, J. (2016). Protecting the Digitized Society — the Challenge of Balancing Surveillance and Privacy. *The Cyber Defense Review, 1*, 75–90.

Hannah-Moffat, K. (2018). Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates. *Theoretical Criminology, 3*, 20–26.

Khasimova, Z. I. (2016). *Criminal and Legal Measures to Counteract Crimes Committed in the Financial Sphere Using Information and Telecommunications Technologies* [Doctoral dissertation]. Krasnoyarsk.

Kravtsov, D. A. (2018). Artificial Intelligence: Crime Prevention and Forecasting. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, *3*, 108–110.

Osipenko, A. L. (2015). New Technologies for Obtaining and Analyzing Operational Search Information: Legal Problems and Prospects for Implementation. *Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia, 2*, 13–19.

Ovchinsky, V. S. (2018). *Criminology of the Digital World*. Textbook for Magistracy. INFRA-M.

Ozhegov, S. I. (1991). *Dictionary of the Russian Language: 70000 Words*. Russian language.

Revier, K. (2018). "Now You're Connected": Carceral Visuality and Police Power on MobilePatrol. Theoretical Criminology.

Spasennikov, B. A. (2018a). *Criminology*: *Medico-Social View*. Publishing House of the Research Institute of the Federal Penitentiary Service of Russia.

Spasennikov, B. A. (2018b). *Criminology: Medical and Social View.* Publishing house of the Research Institute of the Federal Penitentiary Service of Russia.

Sukhodolov, A. P., Ivantsov, S. V., Molchanova, T. V., Spasennikov, B. A., & Kaluzhina, M. A. (2018). Digital Criminology: Mathematical Methods of Forecasting. Part 1. *All-Russian Journal of Criminology, 2,* 230–236.

Sukhodolov, A. P., Kalugina, M. A., Spasennikov, B. A., & Kolodin, V. S. (2019). Digital Criminology: A Method of Digital Profiling of the Behavior of an Unidentified Criminal. *All-Russian Journal of Criminology, 3,* 387.

Yakovets, E. N. (2017). Operational Search Measures of the Police to Ensure the Information Security of the Russian Federation. *Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia, 3,* 127–131.