European Proceedings of
Social and Behavioural Sciences
EpSBS

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

DOI: 10.15405/epsbs.2022.01.87

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

DIGITAL PRESENT AND FUTURE OF FORENSIC SCIENCE

Lyudmila G. Shapiro (a)*, Irina S. Gvozdeva (b), Marina V. Savelyeva (c),
Alexander B. Smushkin (d)
*Corresponding author

(a) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, lyudmila-shapiro2014@yandex.ru
(b) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, gvozdeva-irina@yandex.ru
(c) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, Russia, m300kk64@mail.ru
(d) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, skif32@yandex.ru

Abstract

In recent years the active computerization in all spheres of society has led to digitalization and globalization of crime with new distant methods and mechanisms for committing various types of crimes. This leaves digital footprints of criminal activity in computer memory and other electronic devices and networks, as well as in distributed information storage systems. Electronic digital footprints are left and stored in the memory of information technology devices. The forensic value of distributed storage systems and cloud services is difficult to overestimate. Law enforcement agencies deal with these types of storing information in cases of copyright infringement, as well as illegal distribution of certain content: child pornography, extremist materials, and so on. Blockchain and blockchain-based cryptocurrency (bitcoin) are widely used for illegal financial schemes through the Darknet. Meanwhile law enforcement agencies are often poorly familiar with the feature set of distributed information storage systems. In order to ensure effective counteraction to digital global crimes, activities of law enforcement agencies should be provided with electronic communication technologies. Forensic science, designed to promote a high-quality fight against crime through the development and implementation of various tools, techniques and methods, in this regard, requires a significant digital transformation, which will provide an innovative approach to the detection, investigation and prevention of crimes. All sections of criminology are subject to these changes. These statements prove the relevance of this study, setting theoretical and applied provisions and recommendations aimed at further development of forensic science and improving the effectiveness of countering modern digital crime.

2357-1330 © 2022 Published by European Publisher.

Keywords: Crime investigation, crime prevention, digital criminology, digital footprints, investigative actions

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.15405/epsbs.2022.01.87
Corresponding Author: Lyudmila G. Shapiro
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

During the IV Information revolution, the fast-moving digitalization in all socio-economic and legal spheres of life plays a very important role. Forensic science does not remain aloof, actively accumulating technical, tactical, organizational and methodological innovations. At the same time, it should be noted that certain aspects of digitalization have been reflected in all sections of this science without any exception. The forensic theory and methodology have been supplemented with certain sub-theories related to the specific type of information in technology devices, their systems, networks and its applicability in criminal proceedings.

Russian and foreign scientists presented different versions of these sub theories (Lee, 2001; Rossinskaya, 2019; Spafford & Weeber, 1993). The traditional branch of criminology – forensic tactics or separate investigative action tactic has been also digitalized. So, at present, the tactics of individual investigative actions are conducted either remotely, or with modern software and hardware systems. On the contrary, digital technologies are not easily integrated in "Detection, investigation and prevention of crimes", as into the other branches. Perhaps this is partly due to the nature of this relatively new structural element of forensic science. At the same time, its specific content can be very promising in this regard. The forensic methodology is being actively changed and supplemented with latest components, since the traditional recommendations for the investigation of certain crime categories can no longer meet the needs of combating crime procedures. The crime investigation should be carried out with up to date innovative approach based on the extensive use of information and computer technologies.

2. Problem Statement

In modern conditions, law enforcement agencies need more accurate, detailed and scientific recommendations aimed at ensuring high-quality counteraction to modern crime, which has a digital and global nature. Effective counter measures in forensic science sphere can be based only on new innovative approaches of identifying, disclosing, investigating and preventing certain types of crimes with the help of information and telecommunication technologies.

This approach, first of all, facilitates law enforcement agencies to get necessary digital information array about the circumstances of the committed or impending crime; to analyze the current investigative situation and to choose the most effective investigative direction, considering certain crime methods and footprint picture of a particular crime. In distributed information storage systems and cloud services, information is divided into the smallest information objects that can be mutually downloaded from each other by all participants.

At the same time, at a certain point, no user may have a complete information file. That situation brings out complex questions on how to prosecute a person who owns an incomplete information object; and to find the primary owner of a full information object, who initially posted it in the distributed information storage network, and a number of other difficulties.

3. Research Questions

The main research question is: What are the features of digital changes in forensic theory and practice corresponding to its separate subsections and practical activities?

4. Purpose of the Study

The purpose of study is to look at the current state of digitalization in forensic science, to develop theoretical and practical provisions and recommendations aimed at improving the effectiveness of countering modern crime.

5. Research Methods

The research methods are primarily dialectical, as well as general scientific and logical ones: analysis, synthesis, deduction, induction, and hypothesis. In addition, the research paper actively uses the hermeneutical method to establish the origin of certain concepts and categories and comparative legal analysis of the given issues.

6. Findings

Within the theoretical and methodological framework of forensics, it seems possible to develop a particular theory including collection, research and use of electronic digital information and technology devices. The object of this theory should be the social relations within these spheres. Forensic technology as a branch of criminology is the most promising area studying the big data of distributed and cloud information.

Cloud services can also operate on distributed storage technologies, as well as provide some other variants, such as working through a cloud service, storing databases, using cloud database and so on. Therefore, the specific nature of cloud and distributed storage services works often in practice when the seized suspect’s computer has nothing on it and it is only used as a keyboard with a transmitting device for storing information elsewhere.

Big data has recently taken an increasingly prominent place in the structure of information technology. "Big data" can be understood as an information array characterized by large volumes, high variability and accumulation rate. The sources of "big data" are diverse, for example, sensory data, transaction and administrative one, social network and personal data from tracking devices, etc. (Mayer-Schöenberger & Kookier, 2014). The effective use of this data in the investigation process can help to identify the factors of committed crimes, analyze various crime correlations, which makes it possible to extract new information from the known one with a high degree of probability, to track the relationships and movements of criminals, and prevent terrorist acts.

The remote investigative tactics should also consider the following aspects in its work: the information process structure, its radical changes in variety of information sources, conditions for transmitting information, how information signals are encoded and recoded, and the information capture in this aspect.

Due to the fact that the majority of scientific opinions support the possibility of online interrogation (Internet interrogation, web and videoconference), it seems advisable to recommend drawing up a protocol of this investigative action in the form of an electronic document. It will be signed by the investigator with an enhanced qualified electronic signature, and by other participants - with an electronic signature. The interrogative tactics on in these conditions should include recommendations that provide for the potential possibility of connecting other participants of the interrogation with the help of multi-channel video conferencing: a psychologist, a teacher, an interpreter, a defender, a lawyer, a legal representative of the person being interrogated; as well as resolving the issue of whether they do not need to stay in the same room with the interrogated.

Different distant verbal investigative actions can effectively use video conferencing and computer-mediated reality for the same purposes. But the development of an additional part of forensic tactics is limited by the criminal procedure capabilities. For example, online interrogation tactics should specify the procedural status of a virtual witness – a person who presented the circumstances related to the crime in a remote format using video conferencing systems. Appropriate recommendations for networked interrogation have to include the category of online witness as a person interrogated as a witness in a remote format using software. That is characterized by a sufficient degree of cryptographic security (for example, such universal ones as Skype, WhatsApp, Viber, and so on), and specially developed software and certified electronic interrogation protocol with a digital signature.

Digitalization has influenced the interrogation procedure, including not only the study of the prepared criminal case but also the interrogated person’s account in social networks and messengers. This reference is especially relevant if the age of the person under interrogation is up to 40 years and below. The younger the person is, the greater the amount of video, photo and other data (describing his/her personality helpful in tactical interrogation techniques) can be available to the investigator in open sources via the Internet.

At the present stage of the development in criminology, there is such a specific type of investigative examination as an examination of an account (account in social networks), a user's page in social networks. It should also be noted that the most typical objects of digital inspection are the ones containing electronic digital traces; data on electronic information carriers, for example, in mobile phones, etc. In addition, the object of examination can be both the user's account in social networks, and the mobile device itself, which has personal information, the tactics of which should be improved and include the study of the role by a mandatory participant - a specialist.

The tactical potential of on-site verification of readings is formed taking into account the possibility of its production through videoconferencing, when not all participants are being checked, as well as the use of the computer-mediated reality space, which includes not only virtual, but also other types of reality (Smushkin, 2020), in which the verification will generally take place.

The issue of artificial intelligence usage, an intelligent agent, a police robot, and a cyber investigator has also become relevant for the improvement and development of modern forensic tactics in the digitalization conditions. This is due to the possibility of carrying out certain operations by this intelligence within the framework of specific investigative actions, for example, as it is already happening in the United States, in the Republic of Korea, in Japan, in China, where special computer programs are used that automatically detect and record traces when committing various types of cybercrime, that is, the documentation of electronic traces of cybercrime is carried out not personally by a police detective himself, but by a special computer, digital robot (Kuchin, 2020), and the use of a neural network that functions with the help of forensic thinking basis.

The tactics of remote investigative actions should consider the fact that the structure of information process is radically changing: the sources of obtaining information, the conditions for transmitting information and how the signals are encoded and recoded, what are the features of fixing information in the remote mode and many other aspects.

These proposals cannot but affect the tactic improvement of the considered investigative actions: either by forming separate tactical recommendations, or by forming a separate subsection of forensic tactics – the tactics of remote (using the tools of digitalization of criminal proceedings) investigative actions.

The specific provisions of "Detection, investigation and prevention of crimes" in the forensic literature are also influenced by the use of digital technologies. At the same time, the elements of this subsection can be divided into 3 groups based on the meaning and prospects of using digital technologies in each of them. I. Areas of organizational activity with certain currently used digital aspects: 1) information bases of the investigation; 2) the forensic version; 3) the investigative situation; 4) inquiry program and algorithmization; 5) investigation plan; 6) the study of the individual in criminal proceedings.

II. Areas of organizational activity with attempts of digitalization but inefficient due to national and international research experience: 1) tactical decisions; 2) investigative activities of the inquiry officer; 3) preclusion of the investigation; 4) forensic preventive measures.

III. The perspective directions applying digital technologies from other areas due to the needs of law enforcement agencies. The first group mentioned uses mostly information approach. At the same time, the dataware of judicial proceedings (including criminal ones) is also considered in foreign law enforcement practice (Potas, 1998). It should be noted that there are studies confirming the possibility of adapting artificial neural networks to solve not only typical, but also specific forensic tasks. There are some scientific ideas how to assess tactical risk situations in practice (de-Juan-Ripoll et al., 2018).

As for the second group, it is necessary to talk about tactical decisions. At first sight, the use of artificial intelligence systems seems to be of paramount importance in this matter. At the same time, even the emergence of so-called "intelligent agents" is unlikely to shuffle the burden of making tactical decisions from an official on to artificial intelligence in the nearest future. The third group is connected with forensic forecasting studied by both Russian and foreign scientists (Norton, 2013). In this section, it is also advisable to consider issues related to the information protection from unauthorized access (Bargh et al., 2016), as well as investigative authority identification and authentication accessing information resources.

The main problem of introducing digital technologies within these areas of organizational forensic activity is that systems and software have not yet been developed to account the principles of integrativity and interactivity that underlie them. An example of an attempt to introduce artificial intelligence technology into the activities of law enforcement agencies in 2013-2016 in the United States can serve as an illustration. The interdepartmental experimental program "Artificial Intelligence in the investigation and operational search activities in the commission of criminal offenses" provided for the creation of a paperless police office based on intelligent police assistants with software from IBM and Apple corporations. In July 2016, the program was closed due to unsatisfactory results.

It must be said that due to the dynamically developing technologies, the division proposed by us is conditional. At the same time, it allows to assess the impact of digitalization on investigative activities, as well as to determine those areas where the introduction of these technologies is appropriate.

The changes of forensic methods due to the crime digitalization first of all should be carried out in two main directions. The first is the formation of an independent subsection in the system of general provisions, which should contain recommendations for identification, disclosure, investigation and prevention of crimes committed with the use of information and communication technologies. The second is development of additional elements in the structure of private forensic investigative methods of certain crime categories, which along with traditional methods, can be also committed using digital technologies. These elements will contain data and provisions on a particular crime investigation committed with the use of remote technologies, based on information and computer support. For example, a private forensic methodology should contain digital technology information in forensic analysis that contributes to the certain investigation procedure and variety of investigator’s actions. A promising direction in forensic techniques development is the implementation of cybernetic crime investigative models.

Special attention should be paid to the further development of such a category as forensic crime characterization supplemented with new elements. In its structure, it is advisable to include an additional parameter connected with the remote commission of a particular crime. The forensic crime characteristic in its most general form acts as information model so the differentiation of virtual forensic crime features will be of great practical importance (Rossinskaya, 2019).

The timely crime detection and initiation of criminal proceedings presupposes the cooperation on a digital basis of investigator with regulatory authorities, which, as part of their official activities deal with certain footprints – signs of economic, environmental and other crimes. The implementation of this proposal will ensure, in particular, the rapid information exchange about the crime, the early suppression of criminal activity, the assistance of necessary specialist (expert) in the verification of crime information and its investigation.

7. Conclusion

In conclusion, it is worth noting that the development of a particular theory including collection, research and use of electronic digital information, technology devices or more compact-electronic digital forensics seems to be the most preferable one. It is necessary to work out tactical techniques for remote investigation using modern software and hardware systems, new aspects of general and private forensic techniques that contain proposals for digitally committed crime inquiry and the widespread introduction of information and software into investigative activities. Remote technologies can not only provide high-quality crime control, but also be used in the educational process improving the skills of practitioners.

References

Bargh, M. S., Choenni, S., & Meijer, R. (2016). On design and deployment of two privacy-preserving procedures for judicial-data dissemination. *Government Information Quarterly, 33*(3), 481–493. https://doi.org/10.1016/j.giq.2016.06.002

de-Juan-Ripoll, C., Soler-Domínguez, J. L., Guixeres, J., Contero, M., Álvarez Gutiérrez, N., & Alcañiz, M. (2018). Virtual reality as a new approach for risk taking assessment. *Frontiers in psychology*, *9*, 2532.

Kuchin, O. S. (2020) About some trends in the development of world criminology. In P*roblems of combating crime in the context of digitalization: theory and practice: collection of articles of the XVIII International Scientific and Practical Conference "Criminal Procedure and Criminalistic readings in the Altai"*. Publishing house of the Alt. Uni-ty.

Lee, G. (2001). Computer Forensics: High-Tech Law Enforcement. *IEEE Computer, 34*, 22–27.

Mayer-Schöenberger, V., & Kookier, K. (2014). *Big data. The Revolution that will change the way we live, work, and think.* Mann, Ivanov&Ferber.

Norton, A. (2013). Predictive Policing – The Future of Law Enforcement in the Trinidad and Tobago Police Service. *International Journal of Computer Applications, 62*(4), 32–36. https://doi.org/10.5120/10070-4680

Potas, I. (1998). Informing the discretion: the sentencing information system of the judicial commission of New South Wales. *International Journal of Law and Information Technology, 6*(2), 99–124.

Rossinskaya, E. R. (2019). On the innovative development of forensic science in the era of digitalization. *Legal Bulletin of Samara University, 5*(4), 144–151.

Smushkin, A. B. (2020) The use of computer-mediated reality in law enforcement. *Bulletin of the Tomsk State University, 454*, 251-260.

Spafford, E. H., & Weeber, S. A. (1993). Software forensics: Can we track code to its authors? *Computers & Security, 12*, 585–595.