European Proceedings of
Social and Behavioural Sciences
EpSBS

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

DOI: 10.15405/epsbs.2022.01.103

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

FORENSIC TOOLS OF OBTAINING AND USE OF DIGITAL INFORMATION IN CRIMINAL PROCEDURE

Alexander G. Volevodz (a), Alexander N. Ivanov (b), Evgenyi S. Lapin (c),
Denis S. Khizhnyak (d)*
*Corresponding author

(a) Moscow State Institute of International Relations (MGIMO University), 76, Vernadsky ave., Moscow, 119454, Russia, a.volevodz@inno.mgimo.ru,
(b) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, aivanov@ssla.ru,
(c) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, evgeniy.lapin1961@mail.ru,
(d) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, denis_khizhnyak@mail.ru

Abstract

The article is devoted to the legal and forensic means of remotely obtaining digital information and methodological issues of its use in the investigation of crimes. The problem of obtaining evidence remotely is considered from a broad point of view: the focus is on technologies for remotely obtaining evidence, procedural possibilities and boundaries, comparative analysis of legislation. The research approach is based on a systematic analysis of domestic and foreign legislation, and the practice of investigating crimes in the context of digitalization. According to the results of the study, the authors come to the conclusion that the introduction of digital technologies in criminal proceedings can have a significant impact on the quality of activities of the subjects of investigation and judicial examination of criminal cases. Lack of regulation of the remote formation of evidence in criminal cases using digital technologies entails a lag in the development of new effective technical and forensic tools and methods for the needs of investigation practice by forensic science. The analysis of the assessment of digital evidence in the US criminal proceedings was carried out. It is proposed to use positive legislative developments of American lawyers in the study of digital evidence in Russian legal practice. In this regard, the authors propose to supplement the Criminal Procedure Code of the Russian Federation with Article 182.1 "Search using remote receipt of digital information".

Keywords: Digital information, evidence, forensic science, forensic tools, remote obtaining

https://doi.org/10.15405/epsbs.2022.01.103
Corresponding Author: Denis S. Khizhnyak
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The first decades of the XXI century are characterized by the Digital Revolution – the widespread transition from analogue to digital technologies (Rifkin, 2011). This phenomenon is based on the widespread use of computer technology, comprehensive penetration into all spheres of life, activities of the Internet and other communication networks, robotization, the development of artificial intelligence, and the massive use of telecommunication devices. All this has predetermined the transition of modern society and entire states to "digital reality". According to Russian experts, this phenomenon naturally has a positive overall character (Shestak & Volevodz, 2019).

The digital revolution has brought about more than positive changes. Achievements of scientific and technological progress are also used for criminal purposes. One cannot fail to note the wide spread of crimes in cyberspace, the increase in the number of mercenary crimes committed using computer technologies, computer communications, electronic means of payment (Leukfeldt, 2015) and cryptocurrencies (Sidorenko, 2018), in the use of blockchain technology (Mkrtchian, 2020) causing billions of dollars in damage to the global economy. So, according to Reuters, losses from crime in the field of digital currencies in the first nine months of 2019 alone grew to $ 4.4 billion US dollars, i.e. more than 150% compared to the figures for 2018 as a whole (1.7 billion US dollars) (Chavez-Dreyfuss, 2019).

These circumstances actualize the problem of obtaining and using digital information that has evidentiary value in proving criminal cases.

2. Problem Statement

The era of the digital revolution marked the beginning of the development of new technical and forensic tools and digital vigilantism.

The first step on this path was the introduction into investigative and judicial practice of tactical techniques developed taking into account digital services designed for remote exchange of information in real time.

The most technologically adapted thing for the purposes of criminal proceedings has become a video conference, which allows saving financial resources, promptly receiving forensically significant information in real time.

One of the ways to use this technology in criminal proceedings is the production of procedural actions remotely. In this case, the investigator is physically in one place – the body of preliminary investigation – and the persons and (or) objects under investigation participating in it – in another, at a considerable distance from it. Here we are dealing with the most promising way of using the "man-machine" system. Remote investigation is considered by many to be risky. Without direct contact with the participants (object) of the investigative action, the investigator is limited in the use of tactical means. But we are confident that the remote production of investigative actions will find widespread use in the near future. The practice of preliminary investigation will have to deal with this. The new reality of our time – digital technologies, will force them to be adopted. In support of our forecast, the following arguments can be made.

https://doi.org/10.15405/epsbs.2022.01.103
Corresponding Author: Denis S. Khizhnyak
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

First of all, this type of communication will be accepted in Russian criminal proceedings from the moment convicts held in remand prisons are recognized as having the right to participate in a court of cassation (part 3 of article 376 of the Criminal Procedure Code of the Russian Federation). For the first time in Russia, a court session using videoconferencing took place on November 18, 1999. The huge distances of our country necessitate ultra-long-distance communications.

Second, for about 10 years in the judicial system, interrogation of a witness and a victim has been practiced using videoconferencing systems (part 4 of article 240, part 1 of article 277, article 278.1 of the Criminal Procedure Code of the Russian Federation (hereinafter – the Code of Criminal Procedure of the Russian Federation)). Also, the Code of Criminal Procedure of the Russian Federation provides for the possibility of participating in a court session by using videoconferencing systems for a detained person, in respect of whose property a court of a foreign state has made a decision on confiscation (part 3 of article 473.4 of the Code of Criminal Procedure of the Russian Federation).

Third, even today, in the production of some investigative actions, digital technologies are used, for example, when presenting for identification in order to ensure the safety of the identifying person, excluding his visual observation by means of two computers with connected video cameras in different rooms according to the principle of video conferencing (with one-sided image from the side of placement of identifiable). We believe that in this way it is possible not only to identify living persons, but also the corpse (its parts). This will reduce the psychological tension arising in the production of this type of identification.

Fourth, despite the lack of legal regulation of the procedure for the use of digital technologies at the pre-trial stages of criminal proceedings, the practice of remotely obtaining and using digital information in proving criminal cases is gradually emerging. Thus, the investigator interrogated the victim, who was in a remote settlement, using the Zoom platform. They obtained the necessary testimony, recorded in the protocol of the interrogation of the victim. The protocol was sent to the victim by e-mail. The latter, in turn, through a messenger handed over in a sealed envelope the protocol of the interrogation signed by him and a copy of his passport. The court assessed the protocol of the interrogation of the victim presented by the prosecution as carried out in violation of the criminal procedure legislation. Since the investigator did not interrogate the victim, both at the place of preliminary investigation and at the location of the person being interrogated, including by entrusting such interrogation to another investigator or interrogator. The court made a correct decision in accordance with the Code of Criminal Procedure of the Russian Federation. However, from a forensic point of view, the investigator in this case accelerated and optimized the investigation process.

Fifth, the use of videoconferencing in the interrogation of witnesses and experts in the framework of international cooperation in the field of criminal proceedings is stipulated by a number of international treaties in which Russia participates.

And, finally, foreign experience shows that by the decision of the person conducting the preliminary (pre-trial) investigation, as well as at the request of the person participating in the case, the investigative action can be carried out remotely using digital technologies. In the European Union, the possibility of interrogating a witness, an expert, as well as a suspect or an accused (with his consent) via videoconferencing is provided for by Directive of the European Parliament and of the Council of April 3,

https://doi.org/10.15405/epsbs.2022.01.103
Corresponding Author: Denis S. Khizhnyak
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

2014 No. 2014/41 / EC on the European order for the conduct of criminal investigative actions. In European countries, the practice of interrogating participants in criminal proceedings via video communication has become widespread (for example, in Belgium, Great Britain, Germany, France, Switzerland).

Unfortunately, the domestic criminal procedure law lags behind the realities of today, does not take into account the needs of practice. Although interrogation through the use of video conferencing systems is regulated in a number of articles of the Code of Criminal Procedure of the Russian Federation, their norms are not applicable either to pre-trial proceedings or to international legal assistance in criminal cases.

There is a need to fill this gap by regulating the use of video conferencing for a number of investigative actions.

The spread of computer technology has led to the widespread use of information and telecommunication technologies in the commission of crimes. The legislator reacted quickly enough to this circumstance. The Criminal Code of the Russian Federation currently contains a number of articles in which the use of information and telecommunication networks (including the Internet) is a mandatory element (Art. 159.6; Art. 171.2; Art. 185.3, Art. 274, Art. 282) or a qualifying sign of corpus delicti (clause "d", part 2 of article 110; clause "d" of part 3 of article 110.1; part 2 of article 110.2; part 3 of article 137; cl. “C” part 2 of article 151.2; part 2 of article 205.2; clause “b” of part 2 of article 228.1; clause 1.1 of article 238.1; clause “b” of part 3 of article 242; clause "G" part 2 of article 242.1; item "g" of part 2 of article 242.2; item "g" of part 2 of article 245; part 1.1, item "b" of part 2 of article 258.1; part 3 of article 274.1; part 2 of article 280; part 2 of article 280.1; part 2 of article 282).

The need to obtain and use computer information in proving criminal cases – i.e. information (messages, data) presented in the form of electrical signals (digital traces) made it necessary to inspect computer equipment.

A special rule of law in the criminal procedure law is devoted to working with digital traces – forensically significant information contained on electronic media. This is Art. 164.1 of the Criminal Procedure Code of the Russian Federation, by which the legislator, having determined the exceptional cases in which the seizure of electronic media of information is allowed, established the procedure for the seizure of such media and copying the information contained on them. In general, while positively assessing the emergence of this norm, we believe that this is not enough. It does not fully take into account the possibilities of digital technologies.

Taking into account the need for the practice of collecting digital (electronic) evidence, we consider it necessary to supplement the Code of Criminal Procedure of the Russian Federation, Art. 182.1 "Search using remote digital information retrieval". This article can be summarized as follows:

“An investigator conducting a search of the premises in which a computer system or a separate computer interconnected with it is located, in the presence of sufficient data, believe that information relevant to the criminal case may be stored in another interconnected computer system or part of it. This includes the premises that are physically located in another place within the territory of the Russian Federation, provided that such information can be obtained from the first system or with its help. An investigator has the right to examine all its parts, as well as the information stored in it.

https://doi.org/10.15405/epsbs.2022.01.103
Corresponding Author: Denis S. Khizhnyak
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

The information found is presented to the attesting witnesses, to other persons present during the search, and is copied by a specialist onto electronic media".

An important task of legal scholars is to study and generalize the new and the most important information, which is provided not only by domestic investigative and judicial practice, but also by the experience of foreign law enforcement agencies, courts and legislators related to the provision of remote receipt and use of digital information in proving criminal cases. For instance, let us turn to the US experience we studied.

In the legislation of this country, digital forensic evidence belongs to the category of "scientific evidence", which implies the mandatory participation of a specialist in their research and assessment. There, for a long time, the procedural rule "Fry's standard" was used, according to which the conclusion and testimony of a specialist were taken as an immutable truth. Several considered criminal cases led to a change in legislation and the adoption (without cancelling the previous one) of a new standard for assessing the conclusion and testimony of a specialist – the "Daubert standard".

When looking at the role of specialists and experts according to Fry's rule, their conclusions cannot be considered as one of the evidences, since it is a "scientifically substantiated" verdict issued by specialists (experts) on the basis of studying all the case materials. For example, IT-specialists who base their conclusions on knowledge in the field of information technology are scientific judges according to the "Fry standard", whose verdict is a solution to the issue of special knowledge in a criminal case. An investigator, a judge, a jury cannot critically and scientifically approach the assessment of the opinions of specialists, since this requires a number of scientific knowledge that they do not possess, and therefore they can only follow the competent instructions of specialists. Investigators and judges are independent in choosing specialists, but if they are chosen, the first can only follow their conclusions.

Obviously, the "Frye standard" cancels almost all the main provisions of the law of evidence, the main of which states that the investigator, the court must be critical of the conclusion of an expert and a specialist. According to the Dauber standard, "scientific evidence" is assessed in conjunction with other evidence presented. Moreover, given the complexity of the "scientific evidence", their reliability is determined by the judge during the preliminary hearing. The judge must decide whether the evidence is strong enough to help the jury make decisions, or whether it will only mislead the jury. That is, at this stage, the specialist must clearly, intelligibly explain in simple language the essence of his conclusions. If questions arise in their unambiguous interpretation, then such evidence is not considered by the court.

The US Supreme Court, proceeding from the "Dauber standard", recommended a number of criteria that a judge should be guided by when determining whether evidence should be admitted to trial by a jury or not: 1) whether a research method applied by an expert can be checked or verified; 2) whether the method has been reviewed and published; 3) the potential degree of error (error) of the technique or theory in its application is known either; 4) availability and maintenance of standards and control requirements; 5) the degree of approval of the applied research method (techniques and means) in the scientific community.

In this regard, we consider it not superfluous to consolidate a similar approach to the study of digital traces in one of the guiding clarifications of the Plenum of the Supreme Court of the Russian Federation.

https://doi.org/10.15405/epsbs.2022.01.103
Corresponding Author: Denis S. Khizhnyak
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. Research Questions

3.1. Gaps in Russian legislation regarding the regulation of the remote proof process in criminal cases

Most practitioners and scientists unanimously assert the necessity and advisability of using remote information retrieval in the course of investigative actions. However, the fact that there is still no procedural regulation of the use of this technology suggests that its use is now illegal. Therefore, in the criminal procedure legislation, it is required to provide, first of all, a separate article devoted to the remote collection (formation) of evidence, in which to reflect a number of cases of the expediency of its use.

3.2. System of legal rules required to streamline remote digital generation of evidence

The system of legal norms necessary to regulate the remote digital collection of evidence should consist of a general rule and additions to the existing articles of the criminal procedure law regulating the corresponding investigative actions, reflecting the peculiarities of the use of remote obtaining information for these investigative actions. The general rule should, among other things, reflect the fact that the decision to use remote retrieval of information is made by the investigator (interrogator), and also that it can be applied at the request of the accused, suspect, witness, victim.

4. Purpose of the Study

The purpose of the article is to present scientifically grounded proposals on the legal and forensic support of the process of remote receipt of digital information for the investigation of crimes.

5. Research Methods

The comparative legal research method is applied in the comparative study of individual norms of domestic and foreign criminal procedural laws on the regulation of the remote receipt of evidentiary digital information.

6. Findings

We have considered what remote obtaining of digital information is for proving in criminal cases, why it is necessary and why it is especially important for Russia. Its importance is explained, on the one hand, by its enormous length, and on the other hand, by the presence of developed digital communications and competent personnel for working with digital technologies. In short, there are all the reasons and conditions for the introduction into the practice of preliminary investigation of remote acquisition of digital information (remote collection of evidence).

It is also logical that the nature of digital information is complex. Digital information or digital traces are formed as a result of the interaction of two systems: a person and digital technology with special software. The mechanism or process of digital trace formation is the interaction of these systems that exchange matter, energy and information.

If it were possible in this mechanism to remove information that is not an attribute of the material, but is the moment of the ideal, then it would be possible to classify digital traces as material traces unambiguously. However, this cannot be done with respect to digital footprints. Here the dialectic of the intermediate helps to bring us out of perplexity, according to which, in relation to the extremes (opposites), the intermediate is a synthesis of these opposites. That is: in relation to the opposite - material and ideal traces – digital traces occupy an intermediate position. Digital traces, as an intermediate, are deprivation of both these extremes at the same time or a synthesis of them.

7. Conclusion

The results obtained in this study are in the formulation of legal norms and forensic guidelines for the remote acquisition of digital information.

References

Chavez-Dreyfuss, G. (2019). *Cryptocurrency Crime Surges, Losses hit $4.4 Billion by End-September: Cipher Trace Report*. Reuters. https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-surgeslosses-hit-44-billion-by-end-september-ciphertrace-report-idUSKBN1Y11WH

Leukfeldt, E. R. (2015). Organised cybercrime and social opportunity structures: a proposal for future research directions. *The European Review of Organised Crime, 2*, 91–103.

Mkrtchian, S. M. (2020). Property crimes in the blockchain sphere: new criminal schemes and their criminal law assessment. *Russian journal of criminology, 14*(6), 845–854. https://doi.org/10.17150/2500-4255.2020.14(6).845-854

Rifkin, J. (2011). *The Third Industrial Revolution; How Lateral Power is Transforming Energy, the Economy, and the World*. Palgrave MacMillan.

Shestak, V. A., & Volevodz, A. G. (2019). Modern needs of the legal support of artificial intelligence: a view from Russia. *Russian journal of criminology, 13*(2), 197–206. https://doi.org/10.17150/2500-4255.2019.13(2).197-206

Sidorenko, E. L. (2018). Cryptocrime as a new criminological phenomenon. *Society and Law, 2*(64), 15–21.