Improving electronic evidence legal regulation in criminal proceedings

Ludmila Maiorova*

Siberian Federal University, Law Institute, Svobodnuj 79, Krasnojarsk, 660041, Russia

Abstract. The paper analyzes new sources of information on criminal cases related to digitalization. The study considers the issue on the reasonability of the "electronic evidence" concept introduction into the criminal procedure, the need for additional guarantees of the procedural form of information technologies related evidence. The paper examines the theoretical approaches and requirements, formulated in Russian and European legislation, on the peculiarities of the admissibility of this evidence in criminal cases. Admissibility rules elaboration is a defining moment in this type of information practical use. Another important circumstance is the formulation of the principle of proportionality. The principle of proportionality guarantees the preservation of the fundamental rights of the relevant entities and a system of legal remedies. Much more important is the issue of securing in the current criminal procedural legislation guarantees of observance of the legal rights and freedoms of persons whose interests are affected by obtaining data from various electronic sources in the course of a criminal investigation. Taking into account the invasiveness that accompanies the proper functioning of the new system of comprehensive digitalization, the development of guarantees for the observance and protection of fundamental human rights and freedoms is especially relevant to ensure it. Research reviews German criminal justice experience on this subject matter.

1 Introduction

The emergence of digital technologies in the economy inevitably entails corresponding changes in law. Most often, the concept of electronic evidence is associated with data stored in computer systems or devices, or when it comes to information transmitted electronically over communication networks.

If in the sphere of civil and administrative legislation there are certain processes in this area, then the current criminal procedure legislation is not fully adapted to such sources. Information technologies have been developing quite actively in recent years in Russia, but the problems of introducing digitalization into criminal proceedings have become the subject of scientific research relatively recently. These processes have intensified in connection with the pandemic.

There are diametrically opposite points of view in science about the need for electronic evidence to appear in criminal proceedings as an independent type of evidence.

2 Materials and methods

It should be noted that legal practice develops much faster than legislation, surpasses even theoretical developments in many issues, but needs recommendations based on the generalization of positive experience. This provision can be attributed to various institutions of the criminal procedure, but digitalization related information use will be most relevant in the course of proving. The legal institution in question is at the stage of comprehension and scientific and theoretical justification.

The study uses integral and systemic methods of researching the problem, historical, comparative legal, empirical methods of description, interpretation; theoretical methods of formal and dialectical logic. A legal-dogmatic method and the method of legal norms interpretation were also used.

3 Results

If in the sphere of civil and administrative legislation there are certain processes in this area, then the current criminal procedure legislation is not fully adapted to such sources. Information technologies have been developing quite actively in recent years in Russia, but the problems of introducing digitalization into criminal proceedings have become the subject of scientific research relatively recently. These processes have intensified in connection with the pandemic.

Opinions are diametrically negative, both full recognition and acceptance for electronic evidence. So, L.V. Golovko casts doubt on the radicality of some

* Corresponding author: Lvmaiorova@mail.ru

theoretical approaches and speaks about the absence of the need for the existence of such an independent type (source) of evidence. [1]

S.V. Zuev believes that "despite its essential features, electronic information may well be presented in the form of one of the traditional evidence - material evidence or another document". [2]

Other scholars believe that "the implementation of the idea of transition to the electronic form of a criminal case will require the recognition of electronic information as an independent type of evidence, which will make it possible to consider an electronic document as a kind of this evidence." [3]

S.V. Zuev notes that electronic evidence differs in some properties from an electronic document and material evidence. [4]

O.A. Zaitsev assigns a special role to electronic evidence in the field of criminal proceedings. [5]

Few specialists deny the presence of special specific properties, both in electronic information and in electronic information carriers. V.Yu. Stelmakh singles out distinctive features of electronic information, pointing out that it circulates in the form of electromagnetic pulses and although it has some signs of an "ideal" trace, at the same time it has its own features that are not inherent in their pure form in either "material" or "ideal" traces, since electronic information can be found not on all material objects, but only in the memory of computers and on machine media and when copying electronic information, its original source does not undergo any changes (except when used when copying defective or malicious software), which makes the concepts of "original" and "copy" rather arbitrary in relation to electronic information. [6]

According to P.S. Pastukhov, a new type of evidence ("electronic evidence") or a new source ("electronic media") should not be introduced into the Criminal Procedure Code of the Russian Federation, it is only necessary to clarify the concept of "evidence", indicating that factual data can be in the form of electronic information which in turn, "is quite capable of being perceived in one of the traditional evidence – physical evidence or document". [7]

R.I. Okonenko in his study on electronic evidence comes to a conclusion that it is currently premature to talk about the concept of "electronic evidence" as an established category of positive law, and the appearance of the term "electronic media" in the RF Code of Criminal Procedure should be considered as an intermediate step for the "electronic evidence" term possible appearance in Russian procedural law. [8]

Evidence-based law is one of the central legal institutions of criminal procedural law. The emergence and wide dissemination in practice of new sources of evidentiary information of an electronic (digital) nature have posed questions to science about the necessity and expediency of transmittiong the rules of evidence. Scientific discussions revolve around concepts such as "electronic evidence" and "electronic proof". The range of opinions is quite wide, which indicates the complexity and multidimensionality of the considered phenomena of the new reality.

M.I. Voronin believes that electronic evidence is information contained in an electronic document and / or on an electronic media, on the basis of which the subjects of evidence establish the presence or absence of circumstances to be proven in the course of criminal proceedings, as well as other circumstances, relevant to the criminal case. [9]

The classical basis for dividing evidence by types of sources is the difference in procedural methods of collecting and securing evidence corresponding to the specifics of individual factual data, namely, "the specifics of the method of storing and transmitting information about the essential circumstances of the event under investigation in order to apply such and only such methods of collecting it, which would ensure the completeness and accuracy of the actual data obtained". [10]

Consequently, the specificity of information, stipulating the peculiarities of the collection and consolidation of evidence, predetermines the need to single out one or another type of evidence.

Judicial practice manages to adapt to new realities, investing new meanings in traditional concepts, for example, when not only weapons, but also various media on which information from social networks, the Internet, etc. is transmitted during investigative actions, are recognized as physical evidence. [11]

Passion for technical detailing of the analyzed concepts in criminal procedural law is excessive, it is rather more necessary in forensic science. Despite the widespread use of the term "electronic evidence" in the literature and in practice, many experts express a negative attitude towards the need to single out such evidence as a separate type of evidence and enshrine it in the criminal procedure law.

Determining the reasonability of introducing "electronic evidence" into criminal proceedings is to more extend connected with the regulation of actions and procedures as a result of which digital information can be obtained. The German experience is interesting in these processes comprehension, as they pay more and more attention to new methods of investigation, such as fixing crime traces in the form of digital information, technical control, control of telecommunications, online search and others.

So a lot of modern software uses information encoding that works without any active user actions (for example, WhatsApp). In most cases, information in an encoded form does not fall under the classical form of telecommunications control according to §100a of the Criminal Procedural Code of the Federal Republic of Germany. In this regard, the German legislator developed and introduced the law of August 17, 2017 "On the effective and practice-oriented improvement of the criminal procedure" the so-called "Extension of telecommunications control" (Quellen-TKÜ), which supplemented Paragraph 1 of §100a of the Criminal Procedural Code of the Federal Republic of Germany with proposals 2 and 3.

These provisions allow using technical means to gain access to the information and technical system used by a person, if the classical control of telecommunications is

not possible due to the encoding of information or is associated with disproportionately high costs. Such control is implemented in the form of bypassing device security measures by installing spyware, the so-called "Staatstrojaner", which, in turn, makes it possible to control the current data transfer before it is encoded (at the sender) or immediately after (at the recipient), as well as receive the data of the completed correspondence in case it is saved on the device (for example, WhatsApp or Telegram). As a result, traditional protocols appear in a criminal case, as in a classic telephone conversation.

The law of August 17, 2017, at the last second and without proper discussion along with the rule on "expanding control of telecommunications" also adopted a rule that caused a great resonance in legal circles - the provision on conducting an online search (§100b of the FRG Criminal Procedure Code). [12,13,14]

This provision, in its method, is not much different from "expanding the control of telecommunications", it also says about the "use of technical means", it differs only in the scale of the collected data. So according to Pr. 1 Abs. 1 §100b of the FRG Criminal Procedure Code, law enforcement agencies are allowed, without the knowledge of the persons affected by these measures using technical means to penetrate the information and technical system used by the person and seize data from it.

In view of the exclusiveness of such interference, the conditions for the application of this measure fully comply with the conditions established for acoustic control of a residential premises in accordance with §100c of the Criminal Procedure Code of Germany, namely, a suspicion, based on specific facts, is required that a certain person has committed crimes from the catalog established by law; also, the criminal act is especially grave in a particular case, and the investigation of the circumstances of the case or the establishment of the whereabouts of a person in any other way would be disproportionately complicated or would have no chance of success. At the same time, a closed list of crimes, the so-called "catalog", which included such crimes as crimes against peace, espionage, against state defense, counterfeiting and others, was taken by default from §100c of the German Criminal Procedure Code and moved to §100b Abs. 2 of the Code of Criminal Procedure of the Federal Republic of Germany, which indicates that the online search, in its essence and the degree of interference, corresponds to wiretapping. Thus, in Germany the principle of proportionality operates, that is, on the one hand, a catalog of crimes has been established, on the other hand, the high invasiveness of obtaining digital information is taken into account, that is, a wide range of private information can be collected using information technologies.

Most tools are invasive because they make it possible to have extensive access to personal information, including real-time surveillance, motion detection and other activities such as data from video cameras in public places, as well as methods that reveal traffic data or such as a phone number that was called.

Modern IT technologies contribute to the collection of large amounts of data. This applies to the collection of personal data contained in various sources, such as computers belonging to a suspect or others, or databases containing certain information, such as databases of DNA profiles, fingerprints, etc.

The main common problem is that these IT technologies allow access to an uncontrolled amount of data during an investigation, but on the other hand, are a big problem for protection. This concern is further reinforced by the lack of clear legal provisions for such use in many countries, resulting in a significant degree of police and prosecutorial autonomy in using such methods, accompanied by a relatively low level of judicial oversight.

The principal question facing scientists and practitioners is to what extent traditional procedural guarantees are suitable for adapting to a rapidly changing reality. In particular, when there is no legal regulation, judges have to move to an evolving interpretation of existing constitutional and regulatory provisions. It should be noted that to ensure the effectiveness of the protection of fundamental rights and the monitoring of the investigation, it is necessary the consequences in the event of a violation of such rights to be clearly prescribed by law, or at least predictable. Several new issues related to the aforementioned features of digital evidence do arise with advances in technology, raising concerns about the exercise of the right to protection. The question of determining the conditions and circumstances under which investigative and operational-search actions on access to private digital information can be carried out is quite acute.

It is difficult for the defense to refute the presumption of correctness of any digital information. Part of this task is to verify the authenticity and integrity of the collected data. The other part is related to determining the admissibility of evidence.

A matter that is acute for national law and practitioners is whether there are specific evidentiary rules applicable to digital evidence. On the one hand, they clarified that certain individual rights, although fundamental, are not absolute and can be counterbalanced by other interests. On the other hand, they point to the conditions for a fair invasion of "digital privacy", namely: a) clear, predictable and unambiguous legal provisions allowing access to personal data; and b) proportionality of such access in the sense that it should be the least invasive possible.

It should be noted that this approach is consistent with Article 52 of the EU Charter on Fundamental Rights, which states that “any restriction on the exercise of the rights and freedoms recognized in the Charter must be provided for by law and must respect the essence of the named rights and freedoms. Subject to the principle of proportionality, restrictions may be imposed only when they are necessary and really serve the common interests recognized by the Union, or the need to protect the rights and freedoms of others. "

According to Art. 8 of the European Convention on Fundamental Rights and Freedoms, the interference of public authorities in private and family life must be “in accordance with the law and necessary in a democratic

society in the interests of national security, public security or economic well-being of the country, to prevent disorder or crime, to protect health or morality or to protect the rights and freedoms of others".

The question arises: do the general norms, having been the basis for regulating human rights and freedoms protection for a long time in criminal proceedings retain their significance? Judicial practice is changing, and these changes are connected with ever more advanced digital technologies.

There is an infringement of rights in the name of state sovereignty. The well-known judgment of the European Court of Human Rights "Big Brother Watch v. UK." has caused controversy, in particular, the assertion that mass surveillance per se does not violate the Convention for the Protection of Human Rights and Fundamental Freedoms. [15]

"Big Brother Watch and others against the UK" case can be said to have been a consequence of "Edward Snowden's revelation" about the secret services that used information about personal data to implement an "effective" security system. The complaint to the European Court of Human Rights was about mass interception of messages, intelligence exchange, receiving communication data from communication service providers.

It is possible to say that in the RF Criminal Procedural Code the regulation of actions related to the electronic information acquisition is at the beginning of the path. Probably some of these actions are advisable to regulate in the Law on Operational-Investigative Activities, but there is no doubt that such activities need legislative regulation.

Germany provides guarantees to protect the rights and legitimate interests of persons involved in criminal proceedings. Thus, the control of encoded telecommunication can be assigned to the accused only by the court at the request of the prosecutor's office (§100e Para. 1 Pr. 1 of the Criminal Procedure Code of Germany) or, in exceptional cases, by the prosecutor with subsequent confirmation by the court within 3 days. This measure is also applied to third parties if, by virtue of certain facts, it is reasonable to believe that they are so-called "intermediaries in transmitting information", i.e. transfer or receive messages intended for the accused or outgoing from the accused, or the accused uses their Internet connection.

This measure application to persons entitled to refuse to testify under §53 is limited by §160a and prohibited towards defence counsels under §148 of the German Criminal Procedural Code. The guarantees of the provided actions related to the inviolability and confidentiality of the use of information technology systems are aimed at a high degree of violation of the fundamental rights of a person. At the same time, the German legal community is extremely sensitive about information technology related changes introduced to the Criminal Procedural Code considering them insufficient.

The German experience of the active participation of the prosecutor's office in the supervision of ensuring the legal rights and interests of persons involved in criminal proceedings related to the use of digital technologies can be useful. Further optimization of the activities of the prosecutor's office in criminal proceedings is due to the widespread use of digital technologies, which requires in-depth consideration of the possibility of using specific technological solutions and their safety. [16,17]

It seems that the answer to the main question of concern for judges and scientists: to what extent traditional procedural guarantees are suitable for adapting to a rapidly changing digital reality, will be the following statement. The basic guarantees that are formulated in Article 8 of the European Convention on Fundamental Rights and Freedoms must remain unchanged.

The interference of public authorities in private life must comply with the criteria developed by many years of judicial practice. Certain individual rights, although fundamental, are not absolute and can be counterbalanced by other interests. The high degree of invasiveness in investigations related to the use of digital technologies poses a real threat to personal rights and it is necessary to create protective mechanisms.

Certainly, criminal procedural activities related to digital technologies must comply with the requirements of the law, at the same time, excessive detail should be avoided; it is also necessary to further develop the adversarial nature of the pre-trial proceedings in Russia and ensure access to justice.

4 Conclusion

The issue on whether "electronic evidence" exists and whether it is necessary to introduce this type of evidence seems less relevant than the strict legislative procedure regulation to carry out information technology related actions, and what is even more important, to strengthen the legal rights guarantees of participants in criminal legal proceedings.

It should be added to the above said that the procedural norms of the law of evidence at the present stage must ensure not only the reliability of the information received and used by the subjects of information proof, but also the observance and protection of fundamental human rights and freedoms.

References

1. L.V. Golovko, Digitalization in Criminal Procedure: Local Optimization or Global Revolution? Bulletin of economic security, **1,** 22–25 (2019)
2. S.V. Zuev (ed.), *Fundamentals of the Theory of Electronic Evidence*: Monograph (Moscow, 2019) pp. 253–270.
3. N.A. Golovanova, A.A. Gravina, O.A. Zaitsev et al., *Criminal jurisdictional activity in the context of digitalization:* Monograph (Moscow, 2019) p. 79.
4. S.V. Zuev, Electronic evidence in criminal proceedings: concept and meaning, Law and order: history, theory, practice, **3(26),** 46-51 (2020)
5. O.A. Zaitsev, Features of the Use of Electronic Information as Criminal Evidence: A Comparative-

Legal Analysis of Foreign Legislation, Journal of Foreign Legislation and Comparative Law, **4,** 42-57. (2019). DOI: 10.12737/jflcl.2019.4.4

6. V.Yu. Stelmakh, Electronic information in proving in criminal cases: methods of obtaining and place in the system of evidence, Criminalist Library, **3**, 94–95 (2018)
7. P.S. Pastukhov, On the development of criminal procedural evidence using electronic evidence, in: *The Seventh Perm Congress of Legal Scientists: a collection of scientific articles,* pp. 558-56 (2017)
8. R.I. Okonenko, *"Electronic evidence" and the problems of ensuring the rights of citizens to protect privacy in criminal proceedings: a comparative analysis of the legislation of the United States of America and the Russian Federation:* candidate dissertation (Moscow, 2016)
9. M.I. Voronin, Electronic evidence in the Criminal Procedure Code: to be or not to be? Lex russica, **7** (2019)
10. N.V. Zhogin (ed.), *The theory of evidence in the Soviet criminal procedure*. Ed. 2nd, rev. and add. (Jurid. lit., Moscow, 1973) pp. 257, 635.
11. L.V. Golovko (ed.), *The course of criminal procedure* (Statut, Moscow, 2016) 444 p.
12. Beukelmann, Online search and methods of control over telecommunications, NJW-Spezial, 440 (2017)
13. Roggan, Criminal Procedure Methods of Controlling Telecommunications and Online Search: Measures of Electronic Surveillance of the Defendant and the Society, StV, 82 (2017)
14. Kochheim, Online search and methods of control over telecommunications under the Criminal Procedure Code of the Federal Republic of Germany - legal regulation of deep technical intervention measures under the Code of Criminal Procedure of the Federal Republic of Germany from August 24, 2017, KriPOZ, 60 ff (2018)
15. ECHR. Big Brother Watch and Others v. the United Kingdom. Applications nos. 58170/13, 62322/14 and 24960/15. Judgment of 13 September 2018. URL: http://hudoc.echr.coe.int/eng?i=001-186048
16. H. Putzke, A.N. Tarbagaev, A.D. Nazarov, L.V. Maiorova, The Role of the Prosecutor in the Prevention and Elimination of Investigative Errors: Russian and German Experience, Russian Journal of Criminology, **12**(**3**), 424-430 (2018). doi: 10.17150/2500-4255.2018.12(3).424-430
17. K. Tabolina, V. Tabolin, Prosecutor's Supervision in Criminal Proceedings in the Context of the Leading Development of Digital Relations, Advances in Social Science, Education and Humanities Research, **441,** 376-381 (2020). doi: https://doi.org/10.2991/assehr.k.200526.05