Legal Issues in the Digital Age. 2021. Vol. 2, no. 4.

Research article
УДК 343+341.45
DOI: 10.17323/2713-2749.2021.4.114.129

On the Definition, Legal Essence and Classification of Electronic Information Used Within the Framework of International Cooperation in Criminal Matters

Kirill Klevtsov

MGIMO University, Moscow, Russia, klevtsov001@gmail.com, https://orcid.org/0000-0003-2918-175X

Abstra

The article is devoted to the analysis of such a complex and multifaceted legal phenomenon as „electronic information“. The aim of the research is to define the concept and legal nature of such information. The analysis is based on materialistic dialectics, legal hermeneutics, special and comparative legal methods, a sociological approach and a forecasting method. The study shows that the doctrine and practice lacks a unified approach to understanding electronic information in criminal cases, often the concept of „electronic information“ is confused with „electronic evidence“, while losing sight of its criminal procedural application. Author comes to the conclusion that there is no legislative definition of the concept of “electronic evidence” and it is still possible to operate with the term “electronic information” today, taking into account its cross-disciplinary purpose, respectively, the author’s definition of this concept is proposed. In addition, an attempt was made to determine the types of electronic information in criminal cases, including those requested in the framework of international cooperation, namely, the provision of mutual legal assistance. As an empirical basis for the study, we used the materials contained in the Practical Guide for Requesting Electronic Evidence from Other Countries, prepared jointly by the UN Office on Drugs and Crime, the Executive Directorate of the UN Security Council Counter-Terrorism Committee and the International Association of Prosecutors in collaboration with the EuroMed Justice programs and Euromed Police.

Keywords

electronic information, criminal cases, electronic evidence, international cooperation

For citation: Klevtsov K.K. On the definition, legal essence and classification of electronic information used within the framework of international cooperation in criminal matters. Legal Issues in the Digital Age. 2021, no. 4, pp. 114–129. DOI: 10.17323/2713-2749.2021.4.114.129.

To date, there is no clear understanding both at the doctrinal level and in judicial practice of what "electronic information" is and what is its place in the legal system, including in criminal law. This problem creates serious difficulties in using electronic data as evidence in criminal cases. This seems to be due to the lack of a clear understanding of the comprehensive term "information", which also needs to be clarified taking into account modern realities.

Today's time at the doctrinal level is defined as the "information era" [Churinov N.M., 2002: 10–15], [Raenko S.I., 2013: 189–194], since information [informatio][1] was often of interest both to scientists and to society as a whole. However, until now in philosophy and in other sciences there is no unified approach to understanding the concept of information.

In this regard, the statement of V. Polonskiy, who believes that "the state of the conceptual and terminological apparatus of science allows one to judge the degree of development of the theory corresponding to it, to highlight the various aspects, relationships of real objects and the variety of cognitive tasks ..." [Polonskiy V.M., 1999: 16].

For example, explanatory dictionaries of the Russian language define information as (1) information about the surrounding world and the processes occurring in it, perceived by a person or a special device; and (2) messages informing about the state of affairs, about the state of something.[2] A similar definition is found in jurisprudence dictionaries.[3]

However, this concept is considered differently, depending on the relevant areas of science, which led to the lack of a unified approach. On this score, as it seems to us, V. Vasyukov that this situation is caused by the complex nature of relations based on the theoretical arguments of many sciences: computer science, communication theory, information theory, cybernetics, philosophy, semiotics, information dynamics (the science of open information systems), information science (the science of obtaining, storing and transmitting information for various sets of objects), etc.

[1] From Latin "understanding".

[2] See Ozhegov S.I. (2006) Explanatory dictionary of Russian language. Moscow: Institute of Russian language, RAS; Ushakov D.N. (2014) Explanatory dictionary of modern Russian language. Moscow.

[3] See e.g. Borisov A.B. (2010) Extended legal dictionary. Moscow: Knizhny mir.

[Vasyukov V.F., 2020: 43–44]. From the point of view of informatics, it is a primary concept by analogy with "matter", "energy", as a result of which it cannot be defined through simple categories that have clear boundaries [Bauer F.L., Goos G., 1990: 18]. At the same time, in philosophy, according to the general rule, two theories have been formed — functional and attributive. The first is understood as the fact that information is a product of humanity, therefore, it is cognized only by an individual. According to the second concept, it is matter, along with space and time. [Ursul A.D., 1975: 29], [Afanasyev V.G., 1980: 238].

Today there is a legislative definition of information. According to para. 1 of Art. 2 of the Federal Law of 27.07.2006 No. 149-FZ "On information, information technologies and information protection", information means information any messages or data regardless of the form of their presentation.[4] In the criminal procedure doctrine, attempts have also been made to define information in the context of the theory of evidence. So, for example, V.Ya. Dorokhov meant by it "any information used as evidence in criminal proceedings, having a signal nature" [Dorokhov V.Ya., 1964: 108–117]. At the same time, Professor A.A. Davletov pointed out that information is an element of retrospective cognition, a means by which the subject of cognition establishes the presence or absence of a fact. [Davletov A.A., 1991: 24].

We share the opinion of A.I. Zazulin that in criminal procedural and criminalistic law, participants often encounter analog[5] or discrete[6] information, since it is itself perceived through interrogation, testimony of participants, perception of traces of crime, and the results are denounced either in documents containing the results of operational investigative activities or in the protocols of investigative and judicial actions. [Zazulin A.I., 2018: 79]. At the same time, a special group is made up of electronic information, which has specific features that differ from the ordinary one. In a number of works on criminal procedural law and forensic science, there are similar terms, namely: "machine information"[7], "computer information", "digital information".

It should be noted that the term "machine information" in the criminal law sciences and in the course of the fight against crime, as a general rule,

[4] Collection of Legislative acts of Russian Federation, no. 31 from 31.07.2006 (part I) Art. 3448

[5] An analog signal is a human speech or an image in a photograph.

[6] This is the text, which consists of letters, symbols.

[7] For example, I. Karas proposes to understand it as information circulating in cyberspace, recorded on a physical medium, in a form accessible to the perception of a computer, or transmitted through telecommunication channels [Karas I.Z., 1990: 40].

has been abandoned. This seems to be due to the use of the concept of "computer information" or "computer data"[8] in many legal documents.[9] At the same time, despite the existing international legitimation of this concept, there are still discussions in scientific circles regarding the definition of this phenomenon.

So, A. Kasatkin believes that computer information is factual data that are processed by a computer and obtained at its output in a form that can be perceived by a computer or a person [Kasatkin A.V., 1997: 26]. At the same time V. Krylov understands by it the information, knowledge or a set of commands (programs) intended for use in a computer or controlled by it, located in a computer or on a machine carrier [Krylov V.V., 1997: 27]. A somewhat vague definition, as we see it, is given by N. Zigura. In his opinion, computer information is information that exists in digital form on a physical medium [Zigura N.A., 2010: 28].

Each of the above definitions undoubtedly reflects certain characteristic features of the phenomenon we are considering. However, it is still worth pointing out that the concept of "computer information" in relation to the doctrine of criminal law and criminal procedure has some distinctive features that, it seems, must be taken into account when defining it. At the same time, one should ask an important question, both from a theoretical and practical point of view. The information in smartphones, smart watches, tablets, in the legal sense, refers to computer information, despite the fact that in everyday life these media are a kind of computers.[10] The

[8] Paragraph "b" of Article 1 of the Convention on Cybercrime ETS No. 185, adopted in Budapest on November 23, 2001 (hereinafter — the Budapest Convention), states that "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

[9] According to paragraph "b" of Art. 1 of the Agreement of the Commonwealth of Independent States on combatting crimes in the field of information technology, concluded in Dushanbe, on September 28, 2018, under the computer information is understood the information that is stored in the memory of a computer, on machine or other media in a form accessible to the perception of a computer, or transmitted through communication channels.

Note to Art. 272 of the Criminal Code of the Russian Federation defines this information as information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing and transmission.

It is worth paying attention to the recently introduced operative investigation measure — "obtaining computer information", provided for in paragraph 15 of Art. 6 of Federal Law from 12.08.1995 "On operative investigation activity" (Collection of Legislative acts of Russian Federation (1995), no. 33, Art. 3349).

[10] For example, the „computer" https://en.wikipedia.org/wiki/Computer (accessed 01.12.2021).

information contained in digital cameras, video recorders, robotic vacuum cleaners, etc. is ambiguous in its legal nature. Unfortunately, Russian legislation does not give an unambiguous answer to these questions, as a result of which, we believe, this negatively affects law enforcement.

For example, due to the lack of a detailed procedure for conducting operative investigation measures in the Federal Law "On Criminal Investigation" and the abundance of closed documents, difficulties arise in obtaining information transmitted through instant messaging systems, namely with the help of what type of operational-search measures such data can be obtained? By obtaining information from technical communication channels (clause 11 of article 6) or obtaining computer information (clause 15 of article 6)? To date, this issue remains controversial, despite individual attempts to regulate it in departmental legal acts. In this regard, for example, V. Mescheryakov considers it necessary to abandon the term "computer information", and suggests replacing it with the term "digital object" [Mescheryakov V.A., 2004: 163]

However, some scholars suggest using the term "digital information", taking into account the variety of forms in which such information can exist and be transmitted [Walker C., 2001: 87–88]. For example, N. Ivanov believes that digital information is information recorded on machine media, or transmitted in space in the form of discrete signals — regardless of their physical nature [Ivanov N.A., 2013: 97]. In turn, S. Kushnirenko understands by it information presented in the form of a sequence of numbers available for input, processing, storage, transmission with the help of technical devices [Kushnirenko S.P., 2006: 39]. Some analysts went even further and proposed an original term, considering it an analogue of digital information. This is "information presented in electronic form, which is recorded on machine media, regardless of their physical nature" [Kuvychkov S.I., 2016: 60].

In order not to get bogged down in the discussion, we consider it expedient to use the broader phrase "electronic information" that is applied in law enforcement in criminal cases.[11] Scholars operate with this term as well [Salinovsky K.V., Markelova G.Yu., 2001: 18] [Zaitsev O.A., 2019:

[11] For example, in Art. 1641 of the Code of Criminal Procedure of the Russian Federation refers to the peculiarities of the seizure of electronic media and copying information from them in the course of investigative actions, and in part 7 of Art. 185 of the Code of Criminal Procedure of the Russian Federation uses the terms "electronic messages", "messages transmitted over telecommunication networks." At the same time, the ambiguity of some formulations in these articles is noted in legal doctrine [Vasyukov V.F., 2016: 15–18]; [Shaidullina E.D., Shmeleva O. G., 2018: 44–49]; [Stelmakh V.Yu., 2021: 146–155]. Therefore, proceeding from formal logic, the following conclusion is made that this information is electronic.

42–57] [Pastukhov P.S., 2015: 127–130]. Western lawyers also choose a similar approach in most cases.[12] Electronic information includes various files that contain text, photographs, video recording, sound recording, including those transmitted through the instant messaging system, databases and programs, system files, service utilities and their protocols. Moreover, such information can be located both physically on devices and remotely (for example, in cloud storage).[13] It is obvious that such electronic information can be used in criminal procedural evidence. One of the debatable issues is also the question of the relationship between the concepts of "electronic information" and "electronic evidence". First of all, this is due to the ongoing discussions in general about the concept of evidence [Vyshinsky A.Ya., 1941], [N.V. Zhogin, 1971], [Vladimirov L.E., 2000], [Polyansky N.N., 1946].However, in Russian legislation there is a legal definition of evidence[14], according to which it consists of three elements: (1) factual data (information about facts); (2) sources of factual data; (3) methods and procedure for collecting, consolidating and verifying this factual data. [Balakshin V.S., 2002: 31].

Undoubtedly, the situation with determining the legal nature of electronic evidence is more complicated, as can be seen from the wide range of opinions expressed by lawyers on this issue. Some of them point out that evidence secured in electronic form should be classified as traditional types of evidence. For example, S. Vorozhbit, in the light of civil procedural law, writes that "depending on the type of those electronic data that have evidentiary value, that is, contain information necessary to establish the circumstances of the case, they can be attributed to written, material evidence, audio or video recordings "[Vorozhbit S.P., 2011: 8]. Others believe

[12] See: Strafprozessordnung (StPO) der Bundesrepublik Deutschland. Available at: https://www.gesetze-im-internet.de/stpo/; Code de procédure pénale de France Available at: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/ (accessed: 01.12.2021) etc.

[13] Cloud storage is a model of computer data storage in which the digital data is stored in logical pools, said to be on "the cloud". The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment secured, protected, and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Available at: https://en.wikipedia.org/wiki/Cloud_storage (accessed: 01.12.2021).

[14] According to Part 1 of Art. 74 of the Code of Criminal Procedure, evidence in a criminal case is any information on the basis of which the court, prosecutor, investigator, inquirer, in the manner prescribed by the CCP, establishes the presence or absence of circumstances to be proved in the course of criminal proceedings, as well as other circumstances relevant to the criminal case.

that electronic evidence is a special group within already existing types of evidence, as a result of which they should be given a specific status, taking into account their characteristics. For example, Yu. Sokolov proposes to fix in Art. 81 of the Code of Criminal Procedure of the Russian Federation, a separate wording that allows to recognize as material evidence also information provided in electronic form, which served as an instrument of crime or retained traces of a crime, or at which criminal actions were directed [Sokolov Yu.N., 2010: 116]. It seems that this position is controversial, since it does not differ from the current version of the above article of the Russian criminal procedure law (Article 81). Finally, the third point of view believes that electronic information is a completely new type of evidence, along with others enshrined in Part 4 of Art. 74 of the Criminal Procedure Code of the Russian Federation, since it has specific properties that make them different from other types of evidence [Zagura N.A., Kudryavtseva A.V., 2011: 30].

It should be noted that domestic law enforcement practice classifies the so-called electronic evidence as material evidence, since this is directly provided for by Art. 81 and Art. 84 of the Code of Criminal Procedure of the Russian Federation, as a result of which we share the position of the first group of scholars who classify them as traditional types of evidence. With regard to this problem, R. Okonenko correctly noted that, for example, the appearance of cameras, voice recorders and video cameras, did not lead in the practice of criminal investigation to the classification of information contained in these devices as a special type of evidence [R.I. Okonenko. 2016: 25]. It also did not lead to the emergence of new investigative actions that allowed obtaining such extraordinary evidence. Undoubtedly, it is worth recognizing that there are forensic features of obtaining such electronic information.

Professor L. Golovko discusses this in a very revealing manner. In his opinion, if the protocols of investigative and judicial actions are drawn up in electronic form, then there will be no new "type" of evidence, since the protocols will remain protocols, regardless of the form of their production (handwritten, electronic, etc.). As a result, the cited author comes to the conclusion that there is simply no need for special electronic evidence [Golovko L.V., 2019: 22–25].

Returning to individual aspects of the two previously mentioned terms, we note that some international documents operate precisely with the phrase "electronic evidence".[15] Moreover, in Western legal doctrine, similar

[15] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final — 2018/0108 (COD) // Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed: 01.12.2021); Practical

terminology is used [Moussa A.F., 2021], [Kerr O.S., 2010: 23], [Mason S., 2012: 26–27], [Mason S., 2014: 25–36]. It seems that this is determined by the difference in the legal systems of states, approaches to the definition of evidence and their legal nature. For example, in Common Law countries they use the concept of evidence in a broad sense, without attaching the Russian procedural meaning, as a result of which they legitimately add the word "electronic" to it. For example, in the USA there is no clear differentiation of evidence into types and more emphasis is placed on the formal rights of participants in criminal proceedings when collecting and using evidence in courts [Pizzi U., 21–46], [Burnham U., 2006: 207–216], [Reshetnikova I.V., 1997]. It should be emphasized that the US Federal Evidence Rules, which are a fundamental document in American evidentiary law [Rothstein P.F., 1991: 2], do not contain the concept of "electronic evidence", but use the phrase "electronically stored information".

As Professor O. Zaitsev notes, in most countries of the Continental Law, the admissibility of the use of electronic information is regulated by the general provisions of the legislation on traditional evidence [Zaitsev O.A., 2019: 50].

Without going into serious reflections on this score, we note that today, due to the lack of a normative and doctrinal unambiguous answer to the above question, the phrase "electronic information" should be used, not "electronic evidence". In confirmation of this conclusion, one can also cite the positions of domestic scientists in the field of criminal procedure.

So, M. Strogovich wrote that until the proof is not fixed procedurally, it is not worth arguing that the proof really exists [Strogovich M.S., 1986: 302]. At the same time, Professor S. Sheyfer argued that to recognize the object as evidence, i.e. to introduce it into the process is exclusively the prerogative of the investigating body, the prosecutor and the court, since it is the decision to attach the subject or document to the case that represents the final moment in the formation of evidence [Sheyfer S.A., 1981: 45–46]. Professor V. Balakshin adheres to an approximately similar position [Balakshin V.S., 2004: 94-109]. The same applies to information obtained in the framework of investigation activities, on behalf of the investigator and inquirer[16], as well as in the verification of a crime report (Art. 144 of the

guide for requesting electronic evidence across borders. Vienna: United Nations, 2019.

[16] In the manner prescribed by the Order of the Ministry of Internal Affairs of Russia No. 776, the Ministry of Defense of Russia No. 703, Federal Security Service of Russia No. 509, Federal Protective Service of Russia No. 507, Foreign Intelligence Service No. 42, Federal Penitentiary Servise of Russia No. 535, Federal Drug Control Service of Russia No. 398, Investigation Commetee of Russia No. 68 of September 27, 2013 "On approval of the instruction on the procedure for presenting the results of operative investigation activities to the body of inquiry, investigator or court."

Code of Criminal Procedure of the Russian Federation), which can be considered evidence only after their "procedural assessment". The rationale on this issue is contained in the reasoning of N. Zigura, who believes that the computer information provided by the participants in the criminal process or other persons "will be considered evidence only after the investigator recognizes it as relevant and admissible, and this will happen after reproduction, examination , drawing up a protocol of examination and satisfaction of the petition to attach the carrier of information to the case "[Zigura N.A., 2011: 131].

It follows from this that any electronic information that is de facto evidence in a specific criminal case remains just information until it is collected, verified and evaluated according to the rules of Russian criminal proceedings (Section III "Evidence and proof"). The same argument applies to electronic information in criminal cases obtained in the framework of international cooperation, which will be discussed in more detail below.

Having defined in general terms the terminology and legal nature of electronic information in criminal cases, it is worth moving on to another question that is interesting from a theoretical point of view, but not devoid of its applied purpose. This relates to the problem of the classification of electronic information. This issue was analyzed in detail in the framework of forensic research of digital traces [Meshcheryakov V.A., 2002: 103], [Volevodz A.G., 2002: 159–161], [Kozlov V.E. 2002: 91], [Krasnova L.B., 2005: 25–72], [Smushkin A.B., 2012: 43–48], [Lyanov M.M., 2020: 47–55]. At the same time, the authors of these studies did not touch upon the issues of obtaining electronic information on criminal cases in the context of international cooperation.

So, leaving out the technical and forensic aspects of electronic information, the following classification is proposed.

Depending on the stages of criminal proceedings: (a) obtaining electronic information in the framework of pre-trial proceedings (Part 2 of the CCP RF) and (b) in the course of court proceedings (Part 3 of the CCP RF). At the same time, the receipt of such information in the course of pre-trial proceedings can be both (i) at the stage of initiating a criminal case (Section VII of the CCP RF), and (ii) during the period of preliminary investigation (Section VIII of the CCP RF).[17]

Taking into account the place of its storage: (a) information physically located in the network of national servers (national information resources); (b) information held abroad (extra-territorial information).

[17] Based on the aim of the research, the author analyses exclusively the obtaining electronic information in the framework of pre-trial criminal proceedings.

By its content the electronic information can be (a) publicly available and (b) confidential, i.e. contain state or other secrets protected by law.[18]

From the point of view of the legal basis for receiving electronic information, it can be claimed on the basis of (a) national (domestic) law [19]or (b) the norms of international law.[20]

By subjects. Depending on access to electronic information, such can be (a) individuals who have an electronic storage medium on which such information is stored and who has access to it[21]; (b) the service provider;[22] or (c) the representation of the service provider in another country.

Taking into account the mechanism for obtaining electronic information, it can be classified into information obtained through (a) operational and investigative means, including in the implementation of international police cooperation (for example, police officers sent a request for assistance to law enforcement agencies of foreign states on the basis of intergovernmental agreements or through the National Central Bureau of Interpol), (b) conducting investigative actions (for example, through the sending by the investigator of a request for mutual legal assistance both to the competent authorities of a foreign state and to an entity with access to such information).

Depending on the criminal procedural fate of electronic information. Thus, the data obtained in the framework of international cooperation can

[18] In Russian legislation, such information includes (i) state secrets; (ii) trade secrets; (iii) bank secrecy; (iv) official secrets; (v) professional secrecy (for example, lawyer's, medical), etc. This classification follows from the interpretation of the provisions of the Criminal Procedure Code of the Russian Federation, the Federal Law "On Information"; Law of Russian Federation of July 21, 1993 "On state secrets"; Federal Law of July 29, 2004 "On commercial secrets"; Labor Code of the Russian Federation and various laws providing for service in law enforcement agencies; The Civil Code of the Russian Federation (for example, Art. 857), the Law of Russian Federation of February 12, 1990 "On Banks and Banking Activity", the Federal Law of May 31, 2002 "On the Advocacy and the Bar in the Russian Federation", the Federal Law of December 30, 2008 "On Audit Activity ", The Federal Law of November 21, 2011" On the basics of protecting the health of citizens "; Law of the Russian Federation of July 02, 1992" On psychiatric care and guarantees of the rights of citizens in its provision ", etc. [Popov L.L. 2010: 125–189].

[19] For example, part 4 of Art. 21 of the Code of Criminal Procedure of Russia, clause 31, part 3 of Art. 101 of the Federal Law "On Information".

[20] For example, within the framework of the Budapest Convention, the CIS Convention on Computer Crimes, etc.

[21] Such terminology is enshrined in legislation (for example, Art. 1641 of the Criminal Procedure Code. In addition, according to GOST 2.051-2013, an electronic medium is understood as a material medium used for recording, storing and reproducing information processed using a computer. Electronic information carriers can be used as independent objects (flash drives, memory cards, various removable drives, CD, etc.), and is part of other objects (servers, system units, laptops, video recorders, tablets, mobile phones, etc.).

[22] In this article, it means organizations (companies) providing Internet access services, providing access to a cable network, satellite network, social networking services and transmitting information electronically.

be recognized as (a) material evidence (Article 81 of CCP RF), (b) as other documents (part 2 of Article 84 of the CCP RF) or (c) not recognized as evidence, and returned back to the competent authorities of the foreign state.

It should be noted that within the framework of international cooperation in criminal matters, as a rule, the following types of electronic information are requested.

Basic Subscriber Information. It is the name of the subscriber and may contain information about how long the subscriber has used this particular service, as well as the IP address from which the system was first logged in.

Transactional Information (without content information) — metadata associated with the provision of services. This information includes (a) data related to the connection, traffic, or location of the communication (for example, IP address or MAC address); (b) access logs, which record the time and date of access to the service by a specific individual, as well as the IP address from which the service is accessed; (c) transaction logs, which record a product or service received by a specific individual from a supplier or third party (for example, purchase of cloud storage space).

The content. It represents the text of an email (message), blog or post, video, image or sound stored in digital format (excluding subscriber data or metadata).[23]

Thus, during the criminal prosecution by French law enforcement agencies of terrorist A., who killed two French police officers at their home, it became necessary to obtain the content of the attacker's Facebook accounts on the iPhone, which was seized as part of the inspection of the scene. One account was created in the name of A. and the other in a fictitious name, where he posted a video of the double murder and made a statement about the attack. The French authorities have sent a request for legal assistance regarding the information on both Facebook accounts to the US law enforcement authorities, since the service provider is under the jurisdiction of the US authorities. The latter reported that the good cause standard was met only for an account in a fictitious name due to the posting of a video of the murder, but not for a personal account. An account in a fictitious name has a direct link to the criminal act, whereas a personal account does not.[24]

[23] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. P. 43; See also [Klevtsov K.K., Vasyukov V.F., 2021: 40–41]; [Malov A.A. 2018: 56-60].

[24] Hereinafter, examples from law enforcement practice from the author's personal archive are given, with the exception of those that will be discussed separately.

Conclusion

Today, in law enforcement practice and doctrine, various approaches have been formed to determine the information that is presented in electronic form and is used in the investigation of criminal cases. Various terms are used for its designation, namely: "machine information", "computer information", "digital information", "electronic information", and in some part, and "electronic evidence". Due to the lack of legislative consolidation of these concepts and a unified point of view in theory regarding their legal nature, it is still premature to operate with them (concepts) as established categories.

As we see it, today it is worth starting from a more familiar and laconic term — "electronic information, since it is he who possesses all the necessary features, taking into account its complex and multifaceted criminal procedural essence. Under electronic information in criminal cases (in a broad sense) it is proposed to understand information transmitted by means of any physical signals (usually in electronic form), contained on the appropriate digital media, that is, in a form suitable for human perception, and which are used in the course of criminal proceedings, in particular to establish the circumstances to be proven.

At the same time, one should also take into account the classification of electronic information in the investigation of crimes, depending on: (1) stages of criminal proceedings; (2) the location of the information; (3) its content; (4) legal regulation of its obtaining; (5) its owners; (6) delivery mechanisms; (7) order of its use.

Regarding the implementation of international cooperation in the field of operational-search activities and criminal proceedings, as a rule, the following electronic information is requested: (1) basic information about the subscriber; (2) information about network transactions; and (3) content data.

References

1. Bauer F.L., Gooz G. (1990) *Computer science. Introductory course.* Moscow: Mir, 336 p. (In Russ.).

2. Balakshin V.S. (2002) *Evidence in Russian criminal procedure: concept, essence, classification.* Ekaterinburg: Ural State Law Academy, 112 p. (In Russ.).

3. Balakshin V.S. (2004) *Evidence in theory and practice of criminal procedural proof.* Ekaterinburg: Ural University, 298 p. (In Russ.).

4. Borisov A.B. (2010) Big law dictionary. Moscow: Knizhnyi mir, 848 p. (In Russ.).

5. Burnham U. (2006) *US legal system*. Moscow: Novaya justitsia, 1216 p. (In Russ.).

6. Davletov A.A. (1991) *Basics of criminal procedural knowledge.* Sverdlovsk: University, 152 p. (In Russ.).

7. Dorokhov V.Ia. (1964) The concept of evidence in Soviet criminal procedure. *Sovetskoe gosudarstvo i pravo* = Soviet State and Law, no. 9, pp. 108–117. (In Russ.).

8. Golovko L.V. (2019) Digitalization in Criminal Procedure: Local Optimization or Global Revolution? *Vestnik ekonomicheskoi bezopasnosti* = Herald of Economic Security, no. 1, pp. 22–25. (In Russ.).

9. Idowu S., Capaldi N., Zu L., Gupta A.D. (2013) Encyclopedia of Corporate Social Responsibility. Berlin: Springer: https://doi.org/10.1007/978-3-642-28036-8_100896.

10. Ivanov N.A. (2013) Digital information in criminal proceedings. *Biblioteka kriminalista* = Library of Criminalist, no. 5, pp. 93–102. (In Russ.).

11. Karas' I.Z. (1990) Economic and legal regime of information resources. *Pravo i informatika* = Law and Informatics, no. 2, pp. 40–59. (In Russ.).

12. Kasatkin A.V. (1997) Collecting and using computer information in the investigation of crimes. Candidate of Juridical Sciences Thesis. Moscow, 215 p. (In Russ.).

13. Kerr O.S. (2005) Digital Evidence and the New Criminal Procedures. *Columbia Law Review*, vol. 105, pp. 279–318.

14. Krylov V.V. (1997) *Information computer crimes*. Moscow: Norma, 285 p. (In Russ.).

15. Kushnirenko S.P. (2006) Digital information as an independent object of forensic research. *Vestnik kriminalistiki* = Herald of Criminaltics, no. 2, pp. 43–47. (In Russ.).

16. Kuvychkov S.I. (2016). Use of information presented in electronic form in proving in criminal cases. Candidate of Juridical Sciences Thesis. Nizhny Novgorod, 273 p. (In Russ.).

17. L'ianov M.M. (2020) Modern classification of virtual traces. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniia* = Siberian Criminalistics Transactions, no. 4, pp. 47–55 (In Russ.).

18. Malov A.A. (2018) Obtaining electronic evidence from foreign jurisdictions (United States as a case). *Zakonnost'* = Legality, no. 9, pp. 56–60. (In Russ.).

19. Maslov A.V., Soskova K.A. (2017) Electronic information as evidence in criminal cases. *Tsentral'nyi nauchnyi vestnik* = Central Scholar Herald, no. 11, pp. 57–59. (In Russ.).

20. Mason S. (2014) Electronic evidence: dealing with encrypted data and understanding soft-ware, logic and proof. *Journal of the Academy of European Law,* vol. 15, pp. 25–36.

21. Meshcheriakov V.A. (2004) Electronic digital objects in criminal procedure and forensic science. *Voronezhskie kriminalisticheskie chteniia* = Voronezh Criminalistics Transactions, no. 5, pp. 153–169. (In Russ.).

22. Meshcheriakov V.A. (2002) *Computer information crimes: theory and practice of investigation.* Voronezh: University, 407 p. (In Russ.).

23. Moussa A.F. (2021) Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences,* vol. 11, pp. 1–20. https://doi.org/10.1186/s41935-021-00234-6.

24. Okonenko R.I. (2016). Electronic evidence and ensuring rights of citizens to protect private life in criminal proceedings: a comparative analysis. Candidate of Juridical Sciences Thesis. Moscow, 158 p. (In Russ.).

25. Ozhegov S.I., Shvedova N. Yu. (2006) Explanatory dictionary of the Russian language. Moscow: Temp, 944 p. (In Russ.).

26. Polianskii N.N. (1946) *Evidence in foreign criminal proceedings: modern issues and trends.* Moscow: Yuridicheskoe izdatelstvo, 142 p. (in Russian);

27. Polonskii V.M. (1999) Conceptual and terminological apparatus of pedagogy. *Pedagogika* = Pedology, no. 8, pp. 16–24. (In Russ.).

28. Pitstsi U. (2019) *Litigation Without Truth: Why Our Criminal Trial System Has Become a Costly Error and What We Need to Do to Rebuild It.* Moscow: Infotropik Media, 280 p. (In Russ.).

29. Popov L.L. et al. (2010) *Information Law*. Moscow: Norma, 495 p. (In Russ.).

30. Raenko S.I. (2013) Building information society. *Nauka i sovremennost'* = Science and Modernity, no 20, pp. 189–194. (In Russ.).

31. Reshetnikova I.V. (1997) *The law of evidence in England and the USA.* Ekaterinburg: Ural State Law Academy, 237 p. (In Russ.).

32. Rothstein P.F., Raeder M.S., Crump D. (2012) Evidence in a Nutshell: State and Federal Rules. Minnesota: West Publishing Company, 816 p.

33 .Salinovskii K.V., Markelova G. Uu. (2001) Evidence-based value of electronic information in the Russian criminal process. *Rossiiskii sledovatel'* = Russian Investigator, no. 6, pp. 18–19. (In Russ.).

34. Shaidullina E.D., Shmeleva O.G. (2018) Legislative consolidation of the seizure of electronic correspondence in criminal proceedings. *Vest-*

nik Dal'nevostochnogo iuridicheskogo instituta MVD = Herald of Far Eastern Law Internal Ministry Institute, no. 2, pp. 44–49. (In Russ.).

35. Smushkin A.B. (2012) Virtual traces in forensics. Zakonnost' = Legality, no. 8, pp. 43–48 (In Russ.).

36. Sheifer S.A. (2001) *Investigation. System and procedure.* Moscow: Yurlitinform, 208 p. (In Russ.).

37. Sokolov Yu.N. (2010) *Information technologies in criminal proceedings.* Ekaterinburg: Telekommunikatsionnoe pravo, 418 p. (In Russ.).

38. Stel'makh V.Yu. (2021) The need to change the design of investigative actions aimed at obtaining information transmitted by means of communication. *Vestnik Sankt-Peterburgskogo universiteta MVD* = Herald of Peterburg University of Internal Ministry, no. 1, pp. 146–155. (In Russ.).

39. Strogovich M.S. (1986) *Soviet criminal procedure*. Moscow: Nauka, 470 p. (In Russ.).

40. Ursul A.D. (1975) *Information in modern science. Philosophical essays.* Moscow: Nauka, 287 p. (In Russ.).

41. Vasiukov V.F. (2016) Some issues of conducting investigative actions aimed at detecting, fixing and seizure of electronic messages transmitted through mobile subscriber devices of cellular communication. *Rossiiskii sledovatel'* = Russian Investigator, no. 23, pp. 15–18. (In Russ.).

42. Vasiukov V.F. (2020) Theoretical and legal aspects of crime investigation using subscriber information. Orel: Kartush, 339 p. (In Russ.).

43. Vladimirov L.E. (2000) Doctrine of criminal evidence. Tula: Avtograf. 464 p. (In Russ.).

44. Vorozhbit S.P. (2011) Electronic means of evidence in civil and arbitration proceedings. Candidate of Juridical Sciences Thesis. Saint Petersburg, 235 p. (in Russian);

45. Volevodz A.G. (2002) Countering computer crimes: legal framework for international cooperation. Moscow: Yurlitinform, 485 p. (In Russ.).

46. Vyshinskii A.Ia. (1941) *Theory of forensic evidence in Soviet law.* Moscow: Yuridicheskoe izdatelstvo, 248 p. (In Russ.).

47. Walker C. (2001) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. *Crime Prevention and Community Safety,* vol. 3, pp. 87–88.

48. Zaitsev O.A. (2019) Using electronic information as evidence in a criminal case: a comparative analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = Journal of Foreign Legislation and Comparative Law, no. 4, pp. 42–57. (In Russ.).

49. Zazulin A.I. (2018) Legal and methodological foundations for using digital information as proof in a criminal case. Candidate of Juridical Sciences Thesis. Ekaterinburg, 251 p. (In Russ.).

50. Zhdanko A.V. (2013) *Introduction to General Historiology.* Saint Petersburg: Aleteiya, 277 p. (In Russ.).

51. Zigura N.A. (2010) Computer Information as a type of evidence in criminal procedure in Russia. Candidate of Juridical Sciences Thesis. Chelyabinsk, 234 p. (In Russ.).

52. Zigura N.A., Kudriavtseva A.V. (2011) *Computer information as a type of evidence in the criminal process of Russia.* Moscow: Yurlitinform, 176 p. (In Russ.).

Information about the author:

K.K. Klevtsov — Candidate of Science (Law), Associate Professor.

The article was submitted 10.09.2021; approved after reviewing 22.11.2021; accepted for publication 29.11.2021.