On the using Datamessage as evidence of Cybercrime

A Zharova 1,2 V Elin 1,3

1 National Research University Higher School of Economics. Moscow. Russia
2 Department of Legal Security of the Fuel and Energy Complex, Russian State University of Oil and Gas named after I.M. Gubkin. Moscow. Russia
3 Department of Integrated Safety of Critical Facilities, Russian State University of Oil and Gas named after I.M. Gubkin. Moscow. Russia

E-mail: elin_vm@mail.ru

Abstract. The article reveals a number of features of using computer data in cybercrime cases. The contradictions between the European and Russian approaches to the question of the equivalence of an electronic document and a paper document are considered. The authors reflect the problem of using an electronic document as evidence in criminal cases in compliance with the principle of admissibility of evidence in criminal cases in compliance with the principle of admissibility of evidence in the fight against cybercrime. The paper concludes that there is a need for comprehensive legal and technical regulation of the field of IT relations.

Keywords: IoT; Cybercrimes; Russian procedural law; Electronic document

1. Introduction

More and more public relations are formed using information technology (IT). Not any single developed country can imagine its existence without IT. It is expected that by 2030 “the number of active IoT devices will more than triple and amount to 24.1 billion against 7.6 billion registered at the end of 2019”[1]. This will create a communication system for devices connected to the Internet and transfer large amounts of data. In this regard, the question of the applicability of the technical models to solving the problem of proving cybercrimes is natural. At the level of technical regulation, the problems associated with the development of technologies that meet the requirements of ensuring the integrity and availability of data, reliability, and fault tolerance of information technologies have been solved for a long time. However, there is the problem of the reliability of computer data and it used as evidence in criminal proceedings remains.

With the proliferation of artificial intelligence systems, the number of such issues will increase, since the use of the Internet of Things (IoT), big data technologies used to ensure digital government, and predictive modeling is based on the processing of the information received. In this regard, there is a need to solve the problem of data reliability and information technology reliability.

2. The status of computer information in Russian procedural law

The UNCITRAL Model Law on Electronic Commerce uses the term "Data message", which means information generated, sent, received, or stored by electronic, optical, or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy. Electronic data interchange (EDI)” means the electronic transfer from computer to computer of information using an agreed standard to structure the information [2]. This point of view is also supported by Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000, on certain legal aspects of information society
services, and in particular on electronic commerce in the internal market (Electronic Commerce Directive) [3].

However, Russian law determines that information in electronic form is recognized as an electronic document equivalent to a paper document signed with a handwritten signature only if it is signed with a qualified electronic signature [4][4]. At the same time, initially, an equal sign is not put between an electronic document and a paper document. The conditions determined under which an electronic document can be equated to a written document.

The Convention on Cybercrime [5] contains recommendations for improving procedural legislation and for including computer data in the list of evidence. However, the Russian Federation is ambivalent about the use of the Convention's recommendations.

Firstly, in 2005, Russia explicitly refused to participate in the work of the Convention on cybercrime. When Russia joined Convention, it stated that "the provisions of paragraph b "of article 32 of the Convention is possible to interpret and apply a way that is inconsistent with the purposes and principles of the Convention, and this may harm the sovereignty and national security of States parties and also rights and legitimate interests of their citizens and legal entities."

In this regard, the Russian Federation "can participate in the Convention, subject to a possible revision of the provisions of article 32, paragraph (b) ". The reason for refusing to participate in the joint work was the wording of article 32 "b" that "Party may, without the authorization of another Party access by a computer system in its territory to stored computer data located in another Party, if the Party obtains the legal and voluntary consent of the person who has the legal authority to disclose the data to the Party through that computer system" [6].

Secondly, the norms of the Russian Criminal Code have correlated with the corresponding provisions of the Convention on Cybercrime. For example, the disposition of Art. 159.6 of the Criminal Code of the Russian Federation "Fraud in the field of computer information" actually coincides with the convention's disposition. It should also be borne in mind that the Criminal Code of the Russian Federation includes Chapter 28 "Crimes in the field of computer information." The chapter contains articles providing, including, criminal liability for:

- illegal access to computer information;
- creation, use, and distribution of malicious computer programs
- violation of the rules for operation means of storage, processing, or transmission of computer information (telecommunication networks data).

Thirdly, the Russian Federation does not actually implement the proposals of the Convention on Cybercrime in the field of procedural law. According to the authors, the most significant is the convention's concept of computer data what "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". Concerning this type of evidence, various procedural actions can be performed.

The search and seizure of computer data are aimed at promptly ensuring the safety and partial disclosure of data on information flows. The process includes:

- seizure of a computer system, its part or media used for storing computer data, or in another similar way, ensuring their safety;
- making a copy of the relevant computer data;
- ensuring the integrity of the relevant stored computer data;
- inaccessibility or seizure of computer data located in the computer system.

Collecting data on information flows in real-time provides the ability to:

- collect or record data on information flows using technical means;
- oblige service providers, within the limits of their technical capabilities;
- collect or record using technical means;
- cooperate with competent authorities and help them collect or record in real-time data on information flows associated with specific messages transmitted through a computer system.

Interception of content data in real-time allows:

- collect or record using technical means,
- oblige the service provider, within the limits of his available technical capabilities:
- collect or record using technical means;
- cooperate with the competent authorities and assist them in collecting or recording in real-time data on the content of these messages on its territory, transmitted using computer systems.
Russian Criminal Code understands computer information as information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing, and transmission [11 Art. 272]. The Criminal Procedure Code of the Russian Federation does not directly include computer information in the exhaustive list of admissible evidence [10]. The use of information and computer technologies as evidence is possible if they are categorized as: conclusions and testimonies of experts (specialists), material evidence, or other documents.

According to Federal Law "On Information" an electronic document is documented information presented in electronic form, i.e. in a form suitable:
- for human perception using electronic computers;
- for transmission over information and telecommunication networks;
- for processing in information systems [7, Art.2, p.11-1].

In Russian, documented information is understood as information recorded on a tangible medium by documenting information with requisites that make it possible to determine such information or, in cases established by the legislation of the Russian Federation, its tangible medium. The result of documenting information is a number of legal consequences:
- the expressed subject form of documented information, which allows exercising ownership and other property rights to tangible media containing documented information [8];
- the ability to perform orderly actions in relation to documented information,
- on the perception, use of information, transmission and provision of information during the interaction of various subsystems during storage, processing, and extraction of information
- the presence of certain rules for organizing document flow, creation, provision, storage, and accounting of information carriers;
- the highest efficiency of legal, organizational, and technical protection measures aimed at ensuring the protection of information [9], [10];
- the ability to formulate requirements for the composition of the details of documents and forms of documents; - the existence of requirements for the characteristics of document management systems, including reliability, integrity, complexity and consistency.

3. Electronic document as evidence. Properties and characteristics

The criminal procedure of the Russian Federation determines that proof consists in the collection, verification, and assessment of the evidence in order to establish the event of a crime, the guilt of a person in the commission of a crime, and other significant circumstances [10, Art. 85,73]. The evidence requirements are correlated with the requirements for data security.

In accordance with GOST R ISO / IEC 27000-2012, information security is associated with ensuring the properties of confidentiality, integrity, availability of information, authenticity, accountability, and non-repudiation for the information system [13]. Thus, from a technological point of view, information security is ensured by maintaining confidentiality, integrity, information availability, authenticity, accountability, and non-repudiation. However, the problem of data reliability is not determined, as solving such a problem by technological processes means is a rather difficult task [14].

Reliability is defined as “collecting data from the primary source of information or receiving them from authorities that collect data directly from the primary source of information or organizations that introduce registers with the necessary data if there are data collection standards and their aggregation, as well as the lack of interest of the information source in its content. There is a confirmation that the data has not been changed when performing any operation on them, be it transfer, storage, or publication."

Accuracy is determined through "quality control of data collection and generation, as well as lists of assumptions on the use of the collected data. The description of the data provides for their main characteristics: coverage, collection period, update frequency ".

The completeness of the data is determined through the coverage of data associated with all "counterparties from which information is to be obtained" [15].

It can be concluded that concepts from technical regulation penetrate into the area of legal regulation IT relations.

It should be borne in mind that in 2019 the requirements for ensuring the reliability, integrity, and availability of data in the development of technology for distributed ledger systems were determined. The Ministry of Digital Development, Communications and Mass Media of the Russian Federation signed the “Roadmap for the development of end-to-end digital technology of the Distributed Register System to
ensure the implementation of the strategic directions of state development – “Digital Economy of the Russian Federation” and “Digital Technologies” [16]. There are components of the National Program "Digital Economy of the Russian Federation", which defines the legal requirements for the processes implemented by distributed registry systems [17].

Legal regulation of the reliability of the processed information is associated, among other things, with solving the problem of forming a reliable digital profile of a person [18], and the accuracy of decisions made based on the analysis of the data obtained. In this regard, the methods of legal support for the reliability of data must be investigated in conjunction with the methods of technical assurance of the integrity, security, confidentiality of data, since they determine the parameters of the models for the implementation of technological processes of data processing and the use of information systems, which in turn is associated with ensuring information security [19], [20].

4. Conclusion
In the educational and scientific legal literature, it is argued that the norms of technical regulation and norms of legal regulation are independent areas of regulation. We believe that for the legal regulation of relations arising from the creation and use of IT, this position should be adjusted since the formation of public relations is actually determined by IT developers. And the lack of a coherent system of legal and technical regulation of this sphere of public relations leads to problems of improbability of cybercrimes and, in General, to the problem of ensuring information security.

We can note that the integrity and reliability of the information, the uninterrupted operation of information technology, and its fault tolerance become legal concepts with which the legal regulation of information security is associated. The need to ensure the reliability of data is recognized by the state, but this process requires the involvement of various categories of subjects and the establishment of their rights, duties, and responsibilities, as well as the definition of requirements for the information technologies used for these purposes. To solve this problem, a system of legal regulation in the field of ensuring the reliability of information technologies that process data must be determined. It is also necessary to resolve the issue of amending the criminal procedure legislation of the Russian Federation in connection with the need to include electronic evidence in the list of evidence in criminal cases.

5. Acknowledgments
The reported study was funded by project group of HSE and by RFBR (research project 18029-16013 "Research of conceptual approaches to the formation of a system of legal regulation of information security in the face of great challenges in the global information society").

References
[1] The Number of IOT devices will triple by 2030, Retrieve from https://safe.cnews.ru/news/top/2020-06-30_chislo_ustrojstv_interneta
[2] Model Law on Electronic Commerce of the United Nations Commission on International Trade Law. 1996, Adopted in New York 28.05.1996 - 14.06.1996 at the 29th session of UNCITRAL.
[3] Directive No. 2000/31/EC of the European Parliament and of The Council “On Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce, In The Internal Market”. Retrieve from http://eur-lex.europa.eu/
[4] Federal Law of 06.04.2011 No 63-FZ "On Electronic Signature" The legal reference system" ConsultantPlus".
[5] Convention On Cybercrime (Budapest, 23.XI.2001) Retrieve from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
[6] Order of the President of the Russian Federation of November 15, 2005 N 557-rp "On Signing the Convention on Cybercrime" The legal reference system" ConsultantPlus".
[7] Federal Law No. 149-FZ of 27.07.2006 "On Information, Information Technologies and Information Protection" Collection of legislation of the Russian Federation. No. 31 (1 part), Art. 3448.
[8] Zharova A and Elin V M The Internet of Things in the Russian Federation: Integrated Security Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks. (IGI Global) p 274-290. DOI: 10.4018/978-1-7998-5068-7.ch014
[9] Resolution of the RF Government 28.07.2005 No 452 "About Typical regulations of the internal organisation of Federal enforcement authorities", Collection of legislation the Russian Federation, 01.08.2005, No. 31, Art. 3233
[10] Decree of the Government of the Russian Federation of 19.01.2005 No. 30 "On Standard regulations for interaction of Federal Executive authorities", Collection of legislation of the Russian Federation, 24.01.2005, No. 4, Art. 305.
[11] Criminal Code Russian Federation, The legal reference system "ConsultantPlus”
[12] Criminal Procedure Code of the Russian Federation, The legal reference system "ConsultantPlus”
[13] GOST R ISO / IEC 27000-2012 Information technology (IT). Methods and means of ensuring security. Information security management systems. Overview and terminology The legal reference system "ConsultantPlus”
[14] Andreev A G, Kazakov G V and Koryanov V V 2019 Method for evaluating the reliability of output data prepared by means of an automated system for preparing flight data for aircraft, Engineering journal: science and innovation No 4 (88).
[15] Methodological recommendations for assessing the reliability, completeness and accuracy of data used in calculating performance indicators and the effectiveness of control and Supervisory activities" (approved by the minutes of the project Committee meeting dated 09.11.2017 No. 73 (13)), The legal reference system "ConsultantPlus”
[16] Passport of the National Project "National Program" Digital Economy of the Russian Federation "(approved by the Presidium of the Presidential Council For Strategic Development And National Projects, protocol of 04.06.2019 No 7), Retrieve from https://digital.gov.ru
[17] Zharova A 2020 The protect mobile user data in Russia, International Journal of Electrical and Computer Engineering. vol. 10. No 3. Pp. 3184-3192.
[18] Zharova A 2019 Ensuring the information security of information communication technology users in Russia International Journal of Cyber Criminology. vol. 13. No 2. Pp. 255-269
[19] Chebotareva A A, Chebotarev V E and Rozanov A S 2018 Communication society and security: Current threats and legal maintenance Digital Communication Management. InTech Open Science (Croatia, Spain) pp. 135–182. DOI: https://dx.doi.org/10.15405/epbs.2018.09.02.72.
[20] Chebotareva A A, Danilina E I and Chebotarev V E 2020 Electronic Passports of Citizens as a Personal Essential Attribute During the Pandemic. Proceedings of the Research Technologies of Pandemic Coronavirus Impact (RTCOV 2020). Advances in Social Science, Education and Humanities Research, vol 486. DOI https://doi.org/10.2991/assehr.k.201105.083.