Revista Jurídica vol. 04, n°. 71, Curitiba, 2022. pp. 364 - 380

OPPORTUNITIES FOR USING DIGITAL DATA IN EVIDENCE FOR CRIMINAL CASES

OPORTUNIDADES DE USO DE DADOS DIGITAIS EM EVIDÊNCIA PARA CASOS CRIMINAIS

OPORTUNIDADES PARA UTILIZAR DATOS DIGITALES COMO PRUEBA PARA CASOS PENALES

DMITRY CHIRKOV

Russian State University of Tourism and Service. http:// orcid.org/0000-0001-7257-7157

GENNADY PLOHIH

Southwestern State University. Http:// orcid.org/0000-0002-1407-5834

DARYA KAPUSTINA

Moscow Aviation Institute. Http:// orcid.org/0000-0001-7236-8937

VITALII VASYUKOV

Moscow state Institute of international relations (University); Orel law Institute of the Ministry of internal Affairs of Russia named after V. V. Lukyanov http://orcid.org/0000-0003-0743-5616

ABSTRACT

Objective: the purpose of the study is to determine the reasons that hinder the development of digital elements in evidence in criminal proceedings and detect

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

opportunities for their broader introduction. The authors investigate the current status of the introduction of elements of digitalization in the handling of evidence in criminal proceedings in the Russian Federation.

Methodology: a systematic approach is employed along with a variety of both general scientific and special scientific methods. Information sources are selected and studied using methods of analysis, synthesis, and generalization. The comparative method enables analysis and generalization of international practice in the modernization of criminal proceedings through the digitalization of document flow and handling of evidence and correlation of Russian experience with it. The theoretical and methodological basis of the study is formed by scientific and practical research by Russian and foreign scientists in the field of criminal procedure.

Results: the traditional formalization of criminal proceedings, including the evidentiary process, is greatly complicating the introduction of digital technology today. Specific legal solutions are proposed to allow for the digitalization of the evidentiary process.

Contributions: the discussion of new opportunities offered by modern technology for the needs of fighting and investigating crimes, as well as the risks associated with their use in criminal proceedings.

Keywords: criminal procedure; evidence; evidentiary process; digitalization; digital technology for handling evidence.

RESUMO

Objetivo*: o propósito deste estudo é determinar os motivos que dificultam o desenvolvimento de elementos digitais em provas no processo penal e detectar oportunidades para a sua introdução mais ampla. Os autores investigam o estado atual da introdução de elementos de digitalização no tratamento de provas em processos criminais na Federação Russa.*

Metodologia*: emprega-se uma abordagem sistemática com uma variedade de métodos científicos gerais e científicos especiais. As fontes de informação são selecionadas e estudadas utilizando métodos de análise, síntese e generalização. O método comparativo permite a análise e a generalização da prática internacional na modernização do processo penal por meio da digitalização do fluxo de documentos e manuseio de evidências e sua correlação com a experiência russa. A base teórica e metodológica do estudo é formada por pesquisas científicas e práticas por cientistas russos e estrangeiros no campo do processo penal*

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

***Resultados**: a formalização tradicional do processo penal, incluindo o processo probatório, dificulta muito a introdução da tecnologia digital na atualidade. Em particular, são propostas soluções jurídicas específicas para permitir a digitalização do processo probatório.*

***Contribuições**: a discussão de novas oportunidades oferecidas pela tecnologia moderna para as necessidades de combate e investigação de crimes, bem como os riscos associados ao seu uso em processos criminais.*

***Palavras-chave:** processo penal; provas; processo probatório; digitalização; tecnologia digital para tratamento de provas.*

RESUMEN

***Objetivo**: el propósito del estudio es determinar las razones que dificultan el desarrollo de elementos digitales en la prueba en el proceso penal y detectar oportunidades para su introducción más amplia. Los autores investigan el estado actual de la introducción de elementos de digitalización en el manejo de pruebas en procesos penales en la Federación Rusa.*

***Metodología**: se emplea un enfoque sistemático con una variedad de métodos científicos generales y científicos especiales. Las fuentes de información se seleccionan y estudian utilizando métodos de análisis, síntesis y generalización. El método comparativo permite el análisis y la generalización de la práctica internacional en la modernización de los procedimientos penales a través de la digitalización del flujo de documentos y el manejo de pruebas y la correlación de la experiencia rusa con ella. La base teórica y metodológica del estudio está formada por la investigación científica y práctica de científicos rusos y extranjeros en el campo del procedimiento penal.*

***Resultados**: la formalización tradicional de los procesos penales, incluido el proceso probatorio, complica mucho la introducción de la tecnología digital en la actualidad. En particular, se proponen soluciones legales específicas que permitan la digitalización del proceso probatorio.*

***Contribuciones**: la discusión de las nuevas oportunidades que ofrece la tecnología moderna para las necesidades de lucha e investigación de delitos, así como los riesgos asociados con su uso en los procesos penales.*

***Palabras clave:** proceso penal; prueba; proceso probatorio; digitalización; tecnología digital para el manejo de la prueba.*

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

1 INTRODUCTION

The explosive introduction of digital technologies and digital information in all spheres of human life (Magomedov, 2019) acutely raises questions about their application in various spheres related to the implementation of public authority, especially those that traditionally require strict compliance with the formalities necessary to ensure the rights of all stakeholders (Gavrilov et al., 2022). This to the greatest extent applies to criminal proceedings.

Today, law enforcement officials in their activities to support criminal procedure are actively making use of digital technologies, which allow them to effectively solve and prevent crimes and identify and track down perpetrators (Burova et al., 2021). In this respect, there are a number of peculiar characteristics that complicate the digitalization of the formalities of criminal procedure and the formation of a digital evidentiary base (Rozanova et al., 2020). Lawmakers have left outside the scope of legal regulation a whole range of issues that arise in the course of using digital instruments. The order of using digital means to obtain and present evidence is regulated unclearly. Furthermore, the terminology associated with the handling of digital evidence is not developed (Livson et al., 2021). An opinion is voiced that legislators are underestimating the existing opportunities to effectively use the aforementioned means for obtaining evidence and for the purposes of the evidentiary process in criminal proceedings, as well as the role of digital evidence itself (Tarasov, 2021).

Meanwhile, digital evidence obtained by processing digital traces of crime is now further and further becoming a central element in the investigative process (Kochheim, 2018) thanks to the increased level of cybercrime (Kim, 2017). The rise in cybercrime, in turn, largely owes to the wide use of smartphones and other gadgets, which leads to the generalization of information valuable for law enforcement authorities (Brodovski, Jan 2020) – geolocation data, photos, videos, etc., – by the users (both criminals and victims or third parties).

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Thus, modernization of criminal procedure and its adaptation to the new "digital" reality presupposes not only the digitalization of case management and document flow but also the use of evidence obtained by means of modern information technology (Kirillova et al., 2021). This inevitably presents researchers with the urgency of analyzing the state of regulation of the use of digital evidence in the evidentiary process for gaps in the law.

Law enforcers, legislators, and scholars are now vigorously discussing the new opportunities offered by modern technology for the needs of fighting and investigating crimes, as well as the risks associated with their use in criminal proceedings (Binh, Kien, 2021; Kosevich et al., 2020). Researchers propose various approaches to solving the problems of including digital data as evidence in criminal cases based on the provisions of positivist philosophy (Ishchenko, 2021), correlating the attributive approach in philosophy with the classical theory of evidence (Kartashov, Lesnikov, 2020), and analyzing international experience (Zazulin, 2021). All the suggested approaches are harshly criticized by their opponents, and there is currently no consensus on solving the problems of digitalization of criminal proceedings in sight. Thus, all new studies aimed at addressing the aforementioned issues appear to be quite topical. The purpose of this paper is to investigate the reasons that impede the digital modernization of the criminal process and the possibilities of using international experience in this regard. The hypothesis of the study. Existing criteria for the treatment of evidence, including that obtained by means of digital technology, do not respond to current realities, which requires defining the conditions and limits of the use of new information technology in criminal procedural evidence.

2 METHODS

The systematic approach is employed in the preparation of the article. Along with it, a variety of both general scientific and special scientific methods are used. Information sources are selected and studied using methods of

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

analysis, synthesis, and generalization. The comparative method enables analysis and generalization of international practice in the modernization of criminal proceedings through the digitalization of document flow and handling of evidence and correlation of Russian experience with it. The theoretical and methodological basis of the study is formed by scientific and practical research by Russian and foreign scientists in the field of criminal procedure. The hypothesis of the study is tested using the data of official statistics and other information on the topic available on the Internet. Proceeding from the proposed hypothesis, the special research methods employed in the study are a questionnaire and an expert survey on the reasons for the impeded introduction of digital elements in the evidentiary process in criminal proceedings.

The experts recruited for the study are 33 employees of investigative departments of the Investigative Committee of the Russian Federation in three subjects of the Central Administrative District of the Russian Federation. The experts are selected based on their experience in using digital means in organizing procedural documentation and handling digital evidence, as well as their participation in research activities based on their publication activity in journals cited in Scopus or Web of Science databases, with at least three articles on related topics. The respondents were notified that their responses would be used in this study in a generalized form.

3 RESULTS

Digital data or digital information are currently suggested to be understood in criminal procedure as any information in the form of discrete signals of any physical nature transmitted or stored in information and telecommunications networks or individual devices (media) that is relevant to a criminal case (Kartashov, Lesnikov, 2020). Meanwhile, the law of criminal procedure does not explicitly refer to the possibility of using digitally presented information in criminal proceedings. The lawmaker has chosen to confine

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

themselves to mentioning the term “electronic data carriers” in several articles of the Criminal Procedure Code (CPC) of the Russian Federation (Criminal Procedure Code of the Russian Federation № 174-FZ, December 18, 2001) [8] (Part 4 of Art. 81, Art. 82, Part 8 of Art. 166, Part 9.1 of Art. 182, Part 3.1 of Art. 183 of the CPC of Russia). In reality, the scope of the use of digital information and systems for its processing in criminal proceedings is much broader. For example, digital information processing technology serves as the basis for such investigative actions as the arrest of postal and telegraphic correspondence, its inspection and seizure (Art. 185 of the CPC of Russia), monitoring and recording of conversations (Art. 186 of the CPC of Russia), and obtaining information about connections between users and (or) users’ devices (Art. 186.1 CPC of Russia). In a number of cases, digital technology is used in the course of inspections, searches, examinations, etc. Nevertheless, the vagueness of the terminology in criminal procedure law gives rise to situations in practice where the law enforcer uses concepts “at their discretion”. As rightly noted by A. I. Zazulin (2021), the use of the term “electronic information carriers” in the CPC of Russia leads to an unjustified narrowing of the range of objects that are considered carriers of digital information and in respect of which the seizure with the participation of a specialist and copying of the information contained on them can be carried out.

In the course of the survey, the experts were presented with an open-ended question: “What, in your opinion, are the reasons that make it difficult to use digital data as evidence in criminal proceedings?” The options proposed by the respondents (5) are presented in Table 1 with the percentage distribution of expert opinions on the matter.

Table 1. Reasons complicating the use of digital data as evidence in criminal proceedings

Reason		Distribution of responses, %
1	Vagueness of the concept of digital evidence in law	31
2	Difficulties of converting digital information into analog form	55
3	The possibility of transformation, distortion of digital information during its seizure, fixation, analysis	8

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

4	Inadequacy of the digital form for the existing investigative technology of forming evidence	4
5	Lack of requirements for the technology of storing and presenting digital evidence	2

Meanwhile, in practice, the results of operational-investigative activities (OIA) are in most cases presented in the form of digital information on electronic media. Therefore, during the investigative examination of the electronic digital media, the investigator simply writes down in the protocol part of what they perceived with the senses, that is, what they saw and heard. Translation of electronic information into the content of written protocols of investigative actions, in our opinion, is the essence of the investigative verification of the results of OIA presented in the digital format (Luchinkin, 2021). This is the investigative technology of forming criminal procedural evidence from the results of OIA, presented, among other things, in a digital format. Under this technology, the investigator acts as the main “transformer” of digital information into written information. The criminal procedure system of evidence is based on the investigative standard or, in other words, on the credibility of what is recorded in the protocol of the investigative action. The criterion of admissibility of evidence also largely focuses on the model of the protocol of the investigative action, that is, on compliance with the requirements of Articles 166–167 of the CPC of Russia. This model shapes the notion of “correct evidence” shared by all subjects of evidence, including judges (Luchinkin, 2021). Investigative criminal procedure, with its inherent technology of evidence, is based on the powers of the investigator to form evidence, i.e. to record the information obtained from the protocols of investigative actions and other procedural documents. Investigative technology for the formation of evidence relies on written speech and written speech communication and is not suitable for the digital model of communication: the storage and transmission of digital information. The investigative technology of forming evidence deters the accusatory bias of our criminal justice – this is the main problem with this system. The fact that not all information is subject to digital transformation is an additional, “technological” flaw. The court sometimes detects discrepancies between the content of the protocol of the investigative action and

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

the content of those materials on the basis of which it was created by the investigator, that is, the digital information obtained during the OIA (Adygezalova et al., 2022). In such cases, the judicial investigation goes through direct examination of the "physical evidence", that is, the electronic medium of information received and transmitted to the investigator by the body authorized to carry out the OIA. However, this happens quite rarely. Usually, the results of OIA in the form of digital information are not examined directly, the court is limited to the disclosure of protocols of investigative actions drawn up on the basis of the results of OIA (Federal Rules of Evidence, 2022).

The problem described above raises a logical interest in the evidentiary institutions used in international practice.

In the United States of America, there is no division of evidence into types. What matters is the assessment of the evidence in terms of its admissibility. It appears that for this very reason, there is no debate about the possibility of the existence of "digital evidence" and its place in evidence in criminal cases. The main emphasis is on the observance of rights and legitimate interests in obtaining any evidence, including digital evidence. Rule 101 of the Federal Rules of Evidence (2022) states that written materials include, but are not limited to, information stored electronically. The form in which the written data is presented is irrelevant (rule 1001). The rules also provide a definition of an original and a copy. Whereas for a written document, an original means an analog that has the same meaning for the person who created or executed it, for information stored electronically, an original will be its presentation in a printed or other visually perceivable forms. For copies, the rules make no distinction and define them as the exact reproduction of the original by any method or process (mechanical, photographic, chemical, electronic, or other). As we can see, despite the fact that American legislators make no distinction between "electronic" evidence and ordinary evidence, they still note its specificity.

A number of requirements are imposed on evidence in U.S. criminal proceedings, one of which is reliability. The production of digital evidence in criminal investigations points to a trend away from full acceptance of computer

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

business records because of the complex differences between the records created by a computer, records created by humans but stored on a computer, and records that were digitized and then stored as an archived log file (Jarett et al., 2009). This rule is what determines the complexity, uncertainty, and, ultimately, the admission of evidence in many cases. Digital information for evidence must be authenticated, meaning that it must be verified that it is the same information that was obtained from a particular medium. For all evidence to be admitted, a basis of authenticity must be established, requiring in many cases that witnesses authenticate digital information. The authenticating witness does not necessarily need special qualifications or expert status. All they need to possess is knowledge of the relevant facts to which they testify. However, law enforcement agencies bring in people with special knowledge of digital technology as these kinds of witnesses. This practice is due to the fact that the testimony of a witness who has no understanding of computer technology may not be accepted by the court as evidence of the authenticity of digital evidence (Kartashov, Lesnikov, 2020).

Canadian law not only sets out the rules for evaluating evidence in general but also establishes additional admissibility criteria for electronic documents. Article 31.1 of the Canadian Evidence Act demands authentication of electronic documents, providing that their authenticity can be confirmed by the integrity of the electronic document recording and storage system (Art. 31.3) or by cross-examination under oath (Art. 31.5). The burden of proving the authenticity of an electronic document falls on the person who provides it as evidence (Art. 31.3) (Canada Evidence Act, 1985).

One peculiarity of the evidentiary procedure in French criminal proceedings is the freedom to choose the method of obtaining evidence. At the same time, the investigation body has the right to perform any actions to establish the circumstances of the committed crime. Such specificity, in our opinion, is due to the presence of “free evidence” not bound by the procedural form and not regulated by law (Dudorov, Kartashov, 2017). Articles 706-96 of the CPC of France authorize the investigator to use technical means to obtain digital

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

information placed, stored, and transmitted through telecommunications networks. In this case, such means may not only operate through remote access but also be embedded in the computers or other digital devices of suspects without their consent (Code of Criminal Procedure, 2006). Not only the original digital information seized together with its carrier, but also a copy of such information can be used as evidence in a criminal case (Part 5 of Art. 56, Part 3 of Art. 97 of the CPC of France). As in France, Belgian criminal procedure law does not contain an exhaustive list of types of evidence. Evidence may be given by any means not prohibited by law (Code d' Instruction Criminelle, n.d.). The Belgian CPC pays attention to the peculiarities of the procedure for obtaining digital information. In criminal proceedings, not only provides not only for the seizure of digital information carriers, but also for copying digital information, restricting access to information, or deleting information (Art. 36bis) (Code d' Instruction Criminelle, n.d.). According to the rules laid down in the Belgian CPC, not only one computer network, but also other networks to which the network has access may be searched, if it is necessary to establish the truth in the case or there is a risk of loss of information (Art. 88ter) (Code d' Instruction Criminelle, n.d.). According to Kartashov and Lesnikov (2020), the inclusion of such norms in the Russian law of criminal procedure would partially solve the problem of legal regulation of obtaining digital information stored in "cloud" repositories.

The conducted research allows us to present the features of obtaining digital information in criminal proceedings and its further use in evidence in the form of a comparative table (Table 2).

Table 2. International experience

Countries	Characteristics of the acquisition and use of digital information in criminal proceedings		
	Procedural definition of "Digital Evidence, Digital Devices, Digital Technology" terminology	Procedural regulation of the procedure for obtaining digital evidence	Key procedural criteria for the admissibility of evidence
USA, Canada	Absent	Fragmentary presence	Reliability and authenticity (originality)

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

France, Belgium	Absent	Absent	Integrity, logic, consistency, and clarity
Russia	Fragmentary presence	Fragmentary presence	Formalization of admissibility criteria

Thus, differences found in national legislation and approaches to the regulation of the use of digital information in criminal proceedings in different countries are quite significant. However, the reasons that hinder the introduction of digital technologies in the document flow of criminal proceedings and evidence are similar. These are

- unclear regulation of digital terminology in criminal proceedings.

- the problems of preservation of digital information during its transmission in multistage criminal proceedings.

- technological and material problems of processing large amounts of data.

4 DISCUSSION

The most debatable question in the sphere of using digital information in criminal proceedings is the nature of “digital evidence”. The theory of criminal procedure provides several points of view on this issue. One of them is that digital information is introduced into criminal proceedings by attributing it to traditional types of evidence (physical evidence or other documents). In this line of reasoning, S.P. Vorozhbit (2011) suggests classifying the evidence formed based on digital information based on the classical criterion: if the evidentiary value consists in the physical properties and qualities of the object, such an object or document is to be classified as physical evidence, but if the legal value lies in its semantic content, such an object should be regarded as another document. The position we support is that digital evidence is a new type of evidence along with those described in Part 4 of Art. 74 of the CPC of Russia. Adherents of this point of view note that digital information bears special characteristics that distinguish it from both physical evidence and other documents (Kartashov, 2018). Unlike

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

physical evidence, digital information is immaterial, its volume cannot be defined using physical units. Furthermore, it is the content and not the physical carrier of digital information that has evidentiary value. On the other hand, documents are created by people, whereas digital information is generated only by a set of commands. Documents and physical evidence are immediately available to the human senses, while digital information must be appropriately treated by a special device in order to be perceptible to humans (Zigura, Kudriavtseva, 2011). In addition, it should be noted that today's criminal procedural science has a view that categorically denies the existence of "digital evidence" as such. In particular, A.M. Baranov states categorically that digital evidence is nothing but an illusion, a fantasy of the authors. Moreover, he concludes that the only "source (carrier) of evidence (information) in criminal proceedings is always a person. Evidence-information exists only in the mind of a person; no person – no information". The author goes even further in his reasoning, arguing that "records of investigative actions, expert opinion (in the form of a document), court records, other documents, physical evidence are not the carriers (sources) of information, but the keepers of information" (Baranov, 2019).

This view is hard to agree with. Although digital information can only be transformed into procedural evidence through investigative action, by translating it into a human-perceivable form, there are certain characteristics of digital information that greatly affect its use as evidence in criminal cases.

Therefore, we should concur with the opinion that the need has arisen an objective need to replace the term "electronic data carrier" used in the text of the CPC of Russia with a more broad and appropriate term "digital media", which is to be understood as a material object specifically intended to temporarily and/or permanently storing digital information regardless of the physical principles used for it (Kartashov, Lesnikov, 2020). The introduction of a new group of "digital information" into the list of sources of evidence does not contradict the current law of criminal procedure.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

5 CONCLUSIONS

The conducted research reveals a number of reasons that hinder the adoption of digital technologies in criminal proceedings, including with regard to evidentiary matters, that exist both in Russian and foreign legislation and law enforcement practice. These reasons are largely attributable to the traditional attitude to the criteria of evidence in criminal proceedings in different countries, but a common problem is the lack of a unified theory of digital evidence as a basis for the development of legal terminology and procedural order of treatment of digital evidence. Such a theory would unify the rules for obtaining and further using digital evidence, linking digital technology with the principles of criminal justice. Practical support for this theory should be the training of qualified specialists, including the improvement of digital skills among preliminary investigation officials and judges. Thus, the hypothesis of the study is confirmed. A logical continuation of this study could be a comparative and contrastive analysis of the processes of digitalization in criminal and civil proceedings.

REFERENCES

ADYGEZALOVA, G. E., Dolgov, A. M., Lukozhev, H. M., Faroi, T. V., & Redkovskiy, M. A. (2022). The social role and procedural independence of the investigator in the criminal proceedings of the Russian Federation. JURÍDICAS CUC, 18(1), 217–240. https://doi.org/10.17981/juridcuc.18.1.2022.10

BARANOV, A.M. (2019). Elektronnye dokazatelstva: illiuziia ugolovnogo protsessa XXI v. [Electronic evidence: illusion of the criminal process in the 21st century]. Russian Journal of Criminal Law, 13, 64–69.

BINH, N. H., & Kien, L. T. (2021). Counteraction against digital data leak: Open source software for intrusion detection and prevention. International Journal of Engineering Trends and Technology, 69(3), 17–22. https://doi.org/10.14445/22315381/IJETT-V69I3P204

BRODOVSKI, D., Jan, M. (2020). Tsifrovye dokazatelstva v nemetskom ugolovnom protsesse na stadiiakh predvaritelnogo rassledovaniia, rassmotreniia po sushchestvu i revizii [Digital Evidence in German Criminal Procedure at the

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Stages of Preliminary Investigation, Substantive Review and Revision]. Russian Law: Education, Practice, Research, 3(117), 4-19.

BUROVA, I. L., Volkova, M. A., & Lenkovskaya, R. R. (2021). E-justice in civil cases and economic disputes in the Russian Federation. JURÍDICAS CUC, 17(1), 629–648. https://doi.org/10.17981/juridcuc.17.1.2021.22

CANADA EVIDENCE ACT. (1985). Retrieved from: https://canlii.ca/t/541b5

CODE D' INSTRUCTION CRIMINELLE. (n.d.). Retrieved from: http://www.droitbelge.be/codes.asp#ins

CODE OF CRIMINAL PROCEDURE. (2006). Retrieved from: https://www.legislationline.org/download/id/6381/file/France_CPC_am2006_en.pdf

CRIMINAL PROCEDURE CODE OF THE RUSSIAN FEDERATION № 174-FZ. (December 18, 2001). Retrieved from: http://www.kremlin.ru/acts/bank/17643

DUDOROV, T.D., Kartashov, I.I. (2017). Doznanie kak sokrashchennaia forma predvaritelnogo rassledovaniia: teoriia i praktika [Inquest as a shortened form of preliminary investigation: theory and practice]. Voronezh.

FEDERAL RULES OF EVIDENCE. (2022). Retrieved from: http://www.rulesofevidence.org/

GAVRILOV, B. Y., Voronin, M. Y., Sizova, V. N., Lapin, V. O., & Demidova-Petrova, E. V. (2022). Trends of the criminal-legal complex in relation to the legislative consolidation of the misdemeanor category. JURÍDICAS CUC, 18(1), 183–198. https://doi.org/10.17981/juridcuc.18.1.2022.08

ISHCHENKO, P.P. (2021). Kriterii otsenki sudebnykh dokazatelstv v tsifrovuiu epokhu [Criteria for the assessment of court evidence in the digital age]. Siberian Criminal Procedure and Criminalistic Readings, 1(31), 17-30.

JARETT, H.M., Bailie, M.W., Hagen, E., Judish, N. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved from: https://www.justice.gov/file/442111/download

KARTASHOV, I.I. (2018). Problemy formirovaniia dokazatelstv v ugolovnom sudoproizvodstve na osnove tsifrovoi informatsii [Problems of forming evidence in criminal proceedings on the basis of digital information]. Legal science, 3, 99–103.

KARTASHOV, I.I., Lesnikov, O.A. (2020). Osobennosti polucheniia i ispolzovaniia tsifrovoi informatsii v ugolovnom sudoproizvodstve nekotorykh

zarubezhnykh stran [Specifics of the acquisition and use of digital information in the criminal procedure of some foreign countries]. Vestnik of Voronezh Institute of the Ministry of Interior of Russia, 4, 184-191.

KARTASHOV, I.I., Lesnikov, O.A. (2020). Tsifrovaia informatsiia v ugolovno-protsessualnom dokazyvanii: poniatie i svoistva [Digital information in criminal procedural evidence: concept and properties]. Science. Society. State, 8(4(32)), 73-82.

KIM, H.-K. (2017). Reform of Digital Evidence and Digital Forensic in Korean Criminal Procedure Laws, Sejong: The National Research Council for Economics, Humanities and Social Sciences.

KIRILLOVA, E. A., Zulfugarzade, T. E., Blinkov, O. E., Serova, O. A., & Mikhaylova, I. A. (2021). Prospects for developing the legal regulation of digital platforms. JURÍDICAS CUC, 18(1), 35–52. https://doi.org/10.17981/juridcuc.18.1.2022.02

KOCHHEIM, D. (2018). Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. Munich: C. H. Beck.

KOSEVICH, A. V., Novikova, N. G., Gladkikh, V. I., Sharonin, P. N., & Smirnov, M. A. (2020). Improving economic and legal regulation in the tourism sector. Journal of Environmental Management and Tourism, 11(4), 979–984. https://doi.org/10.14505/jemt.v11.4(44).23

LIVSON, M., Eshtokin, S., Vasyukov, V., Yudina, E., Baybarin, A., Pivneva, S. (2021). Impact of Digitalization on Legal Regulation: formation of new legal practices. Campo Juridico, 9(2). https://doi.org/10.37497/revcampojur.v9i2.749

LUCHINKIN, F.M. (2021). Ispolzovanie rezultatov ORD v vide tsifrovoi informatsii v ugolovno-protsessualnom dokazyvanii [The use of the results of operative-investigative activity in the form of digital information in criminal-procedural evidence], In: 21st Century Technologies in Jurisprudence: proceedings of the 3rd international scientific-practical conference, pp. 427–432. Ekaterinburg: Ural State Law University.

MAGOMEDOV, R.M. (2019). Digital Technologies for Competitive Analysis and Evaluation of Competitive Capacity of a Business Entity. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(1), 1184-1189.

ROZANOVA, E. V., Stepanov, M. M., Alekseev, I. A., Aivazidis, A. K., & Prokoshin, M. S. (2020). History of formation and development of the main legal systems (legal families) in the world. Revista Notas Historicas y Geograficas, (25), 26–36.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

TARASOV, A.V. (2021). Ispolzovanie tsifrovoi informatsii v dokazyvanii pri rassledovanii prestuplenii [The use of digital information in the investigation of crimes]. Scientific Journal “Epomen”, 60.

VOROZHBIT, S.P. (2011). Elektronnye sredstva dokazyvaniia v ugolovnom i grazhdanskom protsesse [Electronic evidence in criminal and civil proceedings]: summary of a candidate dissertation in jurisprudence. Saint Petersburg.

ZAZULIN, A.I. (2021). Tsifrovizatsiia sudoproizvodstva: problemy modernizatsii ugolovnogo protsessa i puti ikh preodoleniia (na primere korolevstva Daniia) [Digitalization of court proceedings: problems of modernization of the criminal process and ways to overcome them (the example of the Kingdom of Denmark)]. Ex jure, 4, 128-140.

ZIGURA, N.A., Kudriavtseva, A.V. (2011). Kompiuternaia informatsiia kak vid dokazatelstva v ugolovnom protsesse Rossii: monografiia [Computer information as a type of evidence in Russian criminal proceedings: a monograph]. Moscow: Iurlitinform.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]