Research article
DOI: https://doi.org/10.21202/jdtl.2023.11

Concept of Electronic Evidence in Criminal Legal Procedure

Anna A. Dmitrieva ✉

South Ural State University (National Research University)
Chelyabinsk, Russian Federation

Pavel S. Pastukhov

Perm State National Research University
Perm, Russian Federation;
Perm Institute of the Federal Penitentiary Service
Perm, Russian Federation

Keywords

Court,
criminal case,
criminal procedure,
digital technologies,
electronic evidences,
electronic interaction,
Information,
investigation,
law,
proving process

Abstract

Objective: elucidating the potential of digital transformation for elaborating the optimal means and methods of collecting evidences and introducing scientific organization of labor of the officials implementing criminal procedure. The scientific approach within the concept consists in minimizing the costs of collecting evidentiary information in criminal cases in electronic form and by electronic means, as well as storing the criminal case materials in electronic form.

Methods: dialectic method occupies the leading position among the research methods, the issues of electronic documentation being considered in the interaction and interdependence with information-technological development of the society. The set of scientific cognition methods within the research creates prerequisites for objective and comprehensive approach to the problems under study.

Results: the authors' concept of electronic evidence is a system of information-technological and legal views on the criminal-procedural form, which is intended for optimizing the process of collecting, registering and preserving them in the criminal case materials. The concept development is aimed at elaborating new approaches to organizing the work of investigation agencies and courts, taking into account the achievements in the sphere of information

✉ Corresponding author

technologies, providing new techniques of collecting criminal-relevant, criminal-procedural, criminological significant information when investigating and hearing of a criminal case. The proposed concept is also aimed at improving interaction and in-service communication of the officials of the preliminary investigation bodies with the officials of information-technological systems for the purposes of collecting evidentiary information in electronic form.

Scientific novelty: the changes were systemically analyzed, which are taking place in the contemporary information society, through the prism of the emerging problems between the sectoral criminal-procedural evidentiary law and more modern technological means of collecting evidentiary information. The article demonstrates a new approach to creating technological interaction using digital technologies, on the scientific base of organization of proving activity, intended to optimize and rationalize the process of proving in criminal procedure.

Practical significance: the research materials can be used to prepare proposals on making changes and additions in the current legislation with a view of implementing the practice of already functioning models of criminal-procedural activity of foreign countries, an inexhaustible potential of information-technologies, software, and artificial intelligence to rationalize proving in criminal cases.

For citation

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Contents

Introduction

The process of proving in criminal cases is predominantly a cognitive sphere of human activity; it has logical content, hence, it operates with multiple theoretical notions, although of great practical significance. A critical role in improving the criminal-procedural proving is played by the notion of evidence, as the criminal procedure is practical activity consisting in collecting, checking and estimating evidences. Like any notion, evidence has its content and volume, i. e. such a set of essential signs, reflected in that notion, so as to provide a law enforcer with the maximally admissible freedom in collecting, checking and estimating them, at the same time possessing the properties of relevance, admissibility and reliability. Establishing the essential signs related to the notion of criminal-procedural evidence requires utmost precision, because in criminal procedure all decisions are made on the basis of evidences, including the decisions on restricting rights and freedoms, guiltiness or guiltlessness. That is why it is inadmissible for such important decisions to be made based on erroneous or false information.

Realizing the importance of essential signs for establishing the restrictive content and volume of the notion of evidence as the basic element of the proving process, we believe that the notion of evidence must be stipulated in law, taking into account the changing conditions of the society development. While digital transformation has changed all basic principles of the society, the law must correspond to the changing conditions. If law, which is conservative by nature, does not change in compliance with the transformation of the society, then a law enforcer will have more and more problems.

The digital transformation of the society that unfolded, the growth of cyber crime, hence the growing evidentiary significance of digital traces of crimes, mass de-facto use of electronic evidences in the practice of law-enforcement agencies – all this is fraught with the problem of the absence of the notion of “electronic evidences” in the criminal-procedural law. Thus, the key objective of the article is to substantiate the need to include the notion of “electronic evidence” into the criminal-procedural law in order to optimize the proving process and increase its efficiency.

We interpret efficiency as the ratio between the resources used and the results obtained. In the information society, the huge volume of electronic information on the modern infrastructure creates difficulties for any person working with information, while at the same time opening great possibilities for investigation agencies. In this regard, a logical question arises: how to achieve maximal result with a minimal amount of power, means, and time. This is the conceptual idea of efficiency in the ratio between the resources used and the results obtained. The authors intend to demonstrate the potential of the information society, reveal the content of electronic evidences in the normative system of criminal-procedural evidences, and formulate the concept of electronic evidence, hence, a more effective proving process. To achieve the set objective, we analyze the trends of electronic evidences development in certain systems of foreign states.

The research was carried out in compliance with dialectic method, which allowed the authors to consider the problem of electronic documentation in interaction with information-technological development of the society.

1. Methods and scientific approaches to the notion of electronic evidences in the Russian law

The ongoing scientific discussion about the notion, essence; features of collecting and preserving; checking electronic evidences testifies to the ambiguous approach to the said aspects. When discussing the issue of introducing the electronic evidentiary information as evidences into criminal procedure, we stated that it can be presented in the classical system of criminal-procedural evidences. Practice shows that electronic evidentiary information is presented in another document, requested from the subjects of information-technological systems, such as information possessor, system administrators, personnel of the information security agencies, Internet providers, communications service providers, personnel of banking and payment systems, operators of video surveillance systems. Often electronic evidentiary information was presented in a material evidence, namely, electronic carriers of information such as smart phones, tablets, notebooks. After expert investigations, such information is presented in an expert's (specialist's) conclusion. We asserted that it is not expedient to change the criminal-procedural legislation in order to include "electronic evidence" as a new type of evidence. We offered an extended interpretation of the current notion of evidences (Pastukhov, 2019). The existing signs of the notion of evidences in the form of "any information", reflected in Article 74 of the Russian Criminal-procedural Code (further – CPC) do not seem to make exceptions for any information. The extended interpretation of the notion of evidences is confirmed by Article 84 CPC, stipulating the consolidation of the evidentiary information not only in the written form ("other documents"), but also on other carriers of information, to which electronic carriers of information may be referred.

We were stemming from the fact that the relative novelty of electronic information, the imperfection of digital infrastructure forced researchers to speak of a new type of "electronic evidence" as a separate criminal-procedural source of evidences. At that, we assumed that with the society adapting to numerous gadgets and information systems the fears regarding electronic information would disappear in and of themselves. This thesis can be traced as each of us masters a smart phone, a computer and their applications. Today, a smart phone in our hands is a bank, a mailing service, a TV, and, actually, a working place. Each of us easily receives information, creates and transfers it, i.e. performs all informational functions. Our thesis is confirmed by the state and corporate trends of abandoning paper money, bank cards, certificated securities, work record and savings books, paper medical records, etc.

Analyzing various views, we may highlight the proponents and opponents of attributing an independent status to electronic evidences. For example, V. G. Golubtsov, objecting to recognition of electronic evidences, writes that electronic-digital technologies do not possess the signs and essential features entailing the need to change the basic institutes of procedural legislation (Golubtsov, 2019).

Denying the self-sustained value of electronic evidence, L. A. Golovko emphasized the absence of novelty (Golovko, 2019), saying that the criminal-procedural category of evidence is much broader and may comprise all electronic data.

Inclusion of electronic evidences into the sphere of proving is advocated by M. I. Voronin (Voronin, 2019). In his opinion, the criminal-procedural legislation should include the notions "electronic evidence", "electronic document" and "electronic carrier of information". The author proposes to take the notion "electronic document" from the Federal Law "On information, information technologies and protection of information"[1]. The main law on information technologies defines an electronic document as documented information presented in electronic form (clause 11.1 of Article 2). We highlight the key sign of an electronic document in the legislative definition – the ability of a human to perceive it using electronic computational devices. This sign is the key one, because during a criminal procedure the readability by humans is of critical importance when working with the complex information-technological environment. Besides, one more sign should be highlighted – the possibility to transfer the electronic document via information-telecommunication networks or to process it in information systems. This legislative definition is extended to any electronic information circulating in the digital environment. Backing up the inclusion of electronic evidences, S. V. Zuev believes that they must meet distinct requirements of admissibility, relevancy and reliability (Zuev & Sutyagin, 2016).

Taking into account the disputability of the notion, essence and prospects of using electronic evidences, we have elaborated a new approach and formulated the concept aimed at information-technological breakthrough in modernizing the criminal-procedural proving and the criminal-procedural activity as a whole. The proposed concept is aimed at separation from the obsolete (archaic) documentary (paper) technique of registering evidences by including the normative interpretation of the notion of "electronic evidences" into the criminal-procedural legislation and accompanying acts. This novelty would resolve the lingering problem of archaic documentary form of certifying evidentiary information and would allow using more advanced, scientifically grounded means of electronically preserving evidentiary information when executing investigation and other procedural actions, or initially request for evidentiary information from the information holders, receive and store it in electronic form. An essential element of the proposed concept is separation

[1] On information, information technologies and protection of information. No. 149-FZ (2006). *Collection of legislation of the Russian Federation*, *31* (Part 1), Article 3448.

of electronic information from the documentary (paper) investigation protocol and electronic carrier of information with the prospect of forming an electronic workflow.

The proposed notion of electronic evidences should provide overcoming the archaic methods when processing electronic evidentiary information and introduce scientific methods of work organization; hence, it is important to reveal not only its potential but also all modern information-technological competitive advantages of electronic means and forms of proving activity. Proposing the said novelties, the authors believe that the electronic form of gathering evidences must provide all the necessary properties and requirements in terms of their reliability and admissibility. Earlier, we have already come to the understanding of the need to stipulate in the criminal-procedural law of the notion of "electronic evidences" in the context of elaborating new approaches to information provision of criminal-procedural activity; we proposed including it into Article 5 of the Criminal-procedural Code in the following edition: "…electronic evidence is juridically significant information registered by electronic means or presented in electronic form, in compliance with the criminal-procedural requirements applied to evidences with a view of establishing the truth in a criminal case" (Pastukhov, 2022a).

The notion of "data" is also of utmost importance, as information society is the "society of data", where information cardinally changes all living conditions, while the speed of information circulation in the digital infrastructure has increased manifold; hence, there is an urgent need to provide a law enforcer with the possibilities to use electronic data without bound to a paper or electronic carrier of information. It follows from the above that we see the solution to the stated problem in eliminating the excessive formalization, in simplifying the criminal-procedural form, elaborating new requirements for admissibility of evidences by developing the concept of electronic data and electronic evidences.

1.1. Notion of electronic evidence in the Russian criminal-procedural legislation

As has been mentioned above, the Russian legislative definition of evidences, being "any information based on which the officials implementing proceedings establish the circumstances subject to proving in the criminal case", is stipulated in Part 1 of Article 74 CPC RF[2]. Such broad interpretation of evidences, allegedly, makes it easy for the preliminary investigation agencies and courts to use evidentiary information in any form, including electronic one.

[2] Criminal-procedural Code of the Russian Federation of 18.12.2001 no. 174-FZ. (2001). *Collection of legislation of the Russian Federation*, *52* (Part I), Article 4921.

However, proclaiming the freedom of collecting evidentiary information in the form of "any information", Part 2 of Article 74 CPC RF limits the list of criminal-procedural sources of evidences as means of proving to seven types: testimony of the suspect, the defendant; testimony of the victim, the witness; conclusion and testimony of the expert; conclusion and testimony of the specialist; material evidences; protocols of investigative and judicial actions; other documents. As can be seen, among the listed criminal-procedural means of proving the electronic data are not mentioned, which is the main problem, creating a contradiction between the traditional conservative investigation model and more modern, hence more effective methods of working with evidentiary information. This contradiction is the main problem of the present article. As was mentioned above, the Russian model of criminal proceedings is an "investigative" one, which means the presence of a separate stage of preliminary investigation, associated with forming evidences in the written materials of a criminal case. The term "preliminary" has two meanings: first, it precedes the stage of judicial procedure, and second, the conclusions of investigation bodies are preliminary. The final conclusions on the guiltiness or guiltlessness are made in court based on the examination of the evidences presented in the criminal case materials.

We generally recognize the importance of the stage of preliminary investigation, when all circumstances of the case are established, while only the criminal cases having distinct judicial prospects are directed to court; however, we consider it necessary to mark the drawbacks of the investigation model, associated with the definition of "evidence". One of the significant drawbacks of the Russian investigation model is its written character, or, to be more exact, its paper form, which impedes effective use of electronic evidentiary information. An investigator forms all criminal case materials as a book, in the protocols of which the data obtained are described in detail, instead of more modern, low-cost means of registering and storing the evidentiary information in an electronic form. This is due to the fact that in the Russian doctrine the main means of registering evidentiary information is description in a protocol. All other means of registration are considered optional, which forces an investigator to describe in detail everything which was already registered in readable form on various carriers of information, or even rewrite what can be seen, i. e. the information from video. For an investigator, the Russian CPC is rather a "guidebook", deviation from which entails abuse of law or inadmissibility of evidences. The investigation model does not allow them to broadly interpret the norms associated with the notion, content and volume of evidences. In the existing legal paradigm and criminal-procedural practice, any evidentiary information, including electronic, must be registered in a written form in the protocol of investigation action, as one of the above listed sources (Part 2 of Article 74 CPC RF).

The identified problem is not solved by the criminal-procedural norm stipulating the collection of evidences in the form of "other documents" (Part 2 of Article 84 CPC RF), which reads that the data may be presented both in written and in another form. These may include photos and films, audio- and video recordings, and other carriers of information.

The problem is not solved by the said norm due to the requirements to a written procedural form of the evidence to provide its admissibility. Besides, "other documents" as a type of evidence are created outside the frameworks of a criminal procedure, but are just attached by an investigator to the criminal case materials. An absolute majority of evidences are formed by an investigator by compiling paper protocols during investigation actions. Although most of the protocols are compiled with computer means, they still must be printed and attached to the criminal case materials in paper form.

Inclusion of the notion "electronic carriers of information" containing digital evidentiary information (Part 4 of Article 81, Parts 1 and 4 of Article 81.1, Article 164.1 CPC RF) into CPC RF in 2012 also does not solve the said problem and does not ensure the efficacy of the activity. The existing requirements to procedural form oblige an investigator to compile a protocol and attach to it the evidentiary information copied on an optical disc. Such approach means manual mode of work and additional expenses. The inadequacy of the manual mode of work becomes even more obvious in the information society, where the digital infrastructure automatically registers a large amount of juridically significant information, which potentially may be criminologically significant and be used as evidence in criminal cases. Collection of such information during proving must take place in an automated mode, but for that, the criminal-procedural law must use the notion of "electronic evidences". The absence of such notion makes the officials implementing proceedings on the case collect evidentiary information in an obsolete, archaic way, storing it in paper protocols. As such order retains, the said contradiction will aggravate, as the volumes of evidentiary information in the digital infrastructure are growing, while human resources are limited.

Although the notion of electronic evidences can be seen in Article 186.1 CPC RF, where the "data on connections" are mentioned, this is just a particular case which does not solve all problems. Data are facts, notions or commands presented in formalized form and enabling their transference or processing both in a manual and automated mode[3].

Further we specify the advantages of introducing the notions of electronic data and electronic evidences into the criminal procedure.

2. Results of conceptual research of the advantages of introducing the notion of electronic evidence

The proposed concept of electronic evidence consists in inclusion of the notions of "electronic data" and 'electronic evidences" into the criminal-procedural law with a view of overcoming the paper mode of registering the criminal case materials. The concept implementation

[3] *GOST R 50922-2006: National standard of the Russian Federation. Information protection. Basic terms and definitions*. (2008). Moscow: Standartinform.

is aimed at optimizing the work with evidences in two directions: first, it will allow collecting evidentiary information from the digital infrastructure electronically; second, it will allow electronically executing investigation and other procedural actions. In both situations, the possibility is provided to register and store the obtained evidentiary information in electronic form in the criminal case materials. We believe that, as a result of this concept implementation, the procedural and material saving of the proving process will occur in the following directions.

1. Inclusion of these notions will allow the officials to not only electronically collect and store evidentiary information without its linking and transferring on an electronic carrier of information, but also register the traditional analog evidentiary information electronically, using computer, audio-, and video means of recording. As is known, collection of evidences is executed in two main modes: 1) by executing investigation actions and compiling respective protocols; 2) by attaching evidentiary information from the modern infrastructure. Today, the banking, payment, navigation systems, communication networks and services, messengers, the Internet information-communication network, video surveillance systems, a lot of Internet-connected things, personal devices accumulate a huge amount of criminologically significant information; thus, attaching of electronic evidentiary information from the listed electronic carriers is prioritized. The electronic means of eviction and attachment of electronic evidentiary information from the above listed devices and systems will cardinally decrease the time for their appropriation.

2. Obtaining of electronic evidentiary information in an integral and unaltered form, instead of a partial description in an investigator protocol, will allow the investigation bodies to obtain an original, which is much more informative than a protocol description. In the Anglo-Saxon system of evidence law there is a best evidence rule, according to which the primary importance is attributed to the original source containing the data about a fact. The best evidence rule, aimed at submitting an original recording to court, is stipulated in Article 1002 of the US Federal rules of evidence[4]. Regarding electronic data, it is stated that standard requirement are applied to them: reliable means of creating and storing the information; reliable means of checking the data integrity; the means of identification of its creator. Examining the original of the electronic information allows additionally revealing the criminological significance of metadata, which allows verifying the document origin, its author, alterations of the electronic document since the moment of its creation to its acquisition by the investigation bodies[5].

3. Obtaining of the electronic information in the original removes contradictions between the evidentiary information in electronic documents and the electronic carriers

---

4 *Federal Rules of Evidence*. (2020). federal_rules_of_evidence_-_december_2020_0.pdf

5 *National standard of the Russian Federation. Providing long-term storage of electronic documents. GOST R 54989-2012/ISO/TR 18492:2005*. (2013). Moscow: Standartinform.

of information. This thesis is important because discussion continues in scientific literature concerning the recognition of electronic information as material evidence (Articles 81, 82 CPC RF) or another document (Article 84 CPC RF). The problem of using an electronic document is not resolved even after attributing a legal status to an electronic document in the courts of general jurisdiction in 2016. Federal Law of June 23, 2016 no. 220-FZ introduced into the Russian Criminal-procedural Code Article 474.1, stipulating the order of using electronic documents in criminal procedure. The parties are entitled to apply to court with petitions, applications, claims, submissions in the form of electronic documents signed with an electronic signature, by filling in a form placed in the official website of the court. By the Order of Judicial Department, the possibility of using an electronic document was detailed in the courts of general jurisdiction[6]. Later the legality of the electronic document status was confirmed by an Enactment of the Plenum of the Supreme Court of the Russian Federation in 2017. According to the above acts of normative interpretation, an electronic document is a document created in electronic form without preliminary documenting on a paper carrier, signed with an electronic signature in the order stipulated by the legislation of the Russian Federation[7]. The said acts introduced the notion of an "electronic image of a document" (electronic copy of a document produced on a paper carrier), i. e. transferred into electronic form by scanning the document produced on a paper carrier, notarized with a simple electronic signature or a qualified electronic signature in compliance with the Order of submitting documents. Despite the said acts explaining the normative interpretation of the necessity to use electronic documents in criminal proceedings, no breakthrough occurred in terms of digitalization of the criminal procedure.

4. Under the development of digital technologies, guarantees have been elaboration against modification of electronic evidentiary information, its integrity, consistency, which are implemented in its copying, duplicating, and calculating the checksum; the requirement to its preservation both at the place of its seizure and in the departmental information system of the infrastructure of law enforcement bodies. One of the most accurate and reliable methods against modification is the calculation of the checksum, i. e. the hash value, which is a bit string with a result output of the hash value[8]. Application of hash values allows compressing electronic documents up to a fixed number of bits, i. e. calculating the unique "dactyloscopic record" of the respective documents, which can

6 Order of Judicial Department under the Supreme Court of the Russian Federation no. 251 of 27.12.2016. (2017). *Bulletin of acts in the judicial system*, *2*.

7 Enactment of the Plenum of the Supreme Court of the Russian Federation no. 57 of 26.12.2017 (2017, December 29). *Rossiyskaya gazeta*.

8 *GOST R ISO/MEC 27037-2014. National standard of the Russian Federation. Information technology. Methods and means of safety provision. Guidelines on identification, collection, receiving and storing of evidences presented in electronic form*. (2014). Moscow: Standartinform.

be used for identification and consistency of information[9]. When checking the evidences, checksums of the original and the copy of electronic evidentiary information are compared, which must coincide for verification. To create and ensure the reliable means of obtaining evidences, the said standard requires storing electronic data with the method based on a 128-bit hashing algorithm MD5, which substitutes an electronic signature with a fingerprint. Criminological significance of the hashing algorithm consists in obtaining a fixed length of the file digital information instead of a discretionary one, which serves as an indentifying property of the electronic document obtained. An additional guarantee of using hash values is storing of the generated record in several copies (two or three) on different electronic carriers of information and on different devices. For example, one copy remains at the holder of the obtained information, similar to a copy of a search protocol, while the second one may be kept of a server of the law enforcement body or on a digital platform. The said technical procedures will comprehensively solve the problems with identification of the obtained electronic evidentiary information.

5. Recognition of the electronic method of recording evidentiary information opens up opportunities and prospects for remote proving. This problem became especially acute during the coronavirus pandemic, quarantine, and isolation. The need to implement justice made electronic online justice almost main direction of development of the Russian legal system. The elements of distant proceedings in criminal cases are already implemented through using video conference systems. Moreover, the video conference technologies are being expanded to procedures at the stage of preliminary investigation. At first, video conferencing was applied solely in appellation (Part 2 of Article 389 CPC RF) and cassation (Part 2 of Article 401 CPC RF) courts, and only for the persons under custody. In the courts of the first instance, video conferencing was applied for considering claims in the order of Article 125 CPC RF and issues related to execution of sentence (Part 2 of Article 399 CPC RF). The most promising were the provisions of CPC RF in terms of using video conferencing in the courts of the first instance for questioning witnesses and victims situated in different settlements (Part 4 of Article 240 CPC RF). We consider the most promising the decision of a Russian legislator to expand the electronic method to perform questioning, face-to-face interrogation, and identification during a preliminary investigation (Article 189 CPC RF) since January 2022.

6. Attributing a legal status to electronic evidence will enable to integrate the information opportunities of managerial, information-technological, operative-investigative, technical-criminological and criminal-procedural activities. Integration of legal branches and types of law enforcement activity will ensure the cumulative effect of criminal-procedural proving. Uniting the information opportunities can be seen in introducing digital platforms

[9] *National standard of the Russian Federation. Providing long-term storage of electronic documents. GOST R 54989-2012/ISO/TR 18492:2005.* (2013). Moscow: Standartinform.

as the most appropriate complex hardware-software solutions to provide interdepartmental electronic interaction of both the criminal prosecuting agencies and all participants of the criminal procedure, defense and court. Through using digital platforms, a new form and content of automated information interaction are created, which compensate for the languidness of a human factor. The digital technology of communication of the preliminary investigation authorities with the information system officials increases the speed of information exchange and facilitates feedback between the bodies and officials (Zaytsev & Pastukhov, 2019). Examining the practice of law enforcement bodies shows trends towards creating digital platforms: Ministry of Internal Affairs, Prosecutor's Office, Defense Attorneys, to say nothing of corporate organizations. The use of digital platforms must transform paper record-keeping into an electronic document flow.

7. Inclusion of the "electronic evidence" notion opens up the prospects for using artificial intelligence, big data, video analytics and video semantics (Zaytsev et al., 2021; Pastukhov, 2022b; Reedy, 2023; Horsman, 2023; Wu & Zheng, 2020; Chen et al., 2020) as most rational automation methods of collecting evidences. The artificial intelligence combined with digital platforms opens up a new epoch of automation and robotization in proving activity in terms of collecting evidences from communication networks, navigation systems, information systems and databases. Automated examination of various databases will largely increase the information-analytical opportunities of criminological registration, accounting of police and other law enforcement bodies, enabling to process great volumes of data through a set of approaches, tools and methods of automated processing of structured and unstructured information coming from a large number of various sources, including discrete or loosely-coupled, in the amount which are impossible to process in manual mode in a reasonable time (Horsman, 2021).

8. Due to electronic evidences, proving will become a process of identification of a personality (de Hert et al., 2018), information-technological devices, people's actions, events, and results. Identification will take place by digital methods based on digital identifiers, digital face profiles (Hoile et al., 2011), digital platforms, interdepartmental electronic interaction system, accounting of criminological registration and other types of automated registration.

9. Using the Uniform system of identification and authentication, which has proved its efficiency in the recent decade, with a view of introducing digital platforms for interdepartmental interaction of law enforcement bodies and courts for user identification[10]. By now, a more effective system has been developed – a uniform biometric system providing processing, including collection and storage, of biometric personal data, their checking and transfer of information about the correlation to the submitted biometric personal

[10] Enactment of the Government of the Russian Federation no. 584 of 10.07.2013. (2013). *Collection of legislation of the Russian Federation*, *30* (Part II), Article 4108.

data of a physical person with a view of identification and authentication of the physical person[11]. The uniform biometric system using information technologies enables to most quickly identify a person by unique physical signs such as DNA, face, fingerprints, voice, signature, and identity papers (Zaytsev & Pastukhov, 2022).

10. Using of electronic evidences opens up the prospects for forming an information-technological mode of proving, new strategies of crimes investigation and solving (Wu & Zheng, 2020). Establishing the new mode testifies to the transition "from documents to data", transferring paper document flow into the digital form. In the new digital mode of the society, a promising technology of document flow is the blockchain technology, based on the principle of context dependency. The use of this technology ensures verity, reliability, inalterability and safety of electronic documents.

11. At the stage of litigation during court investigation, checking of electronic evidences is provided by visualizing the evidentiary information using computer, audio- and video means by all participants of the litigation, not only the state prosecutor holding the paper materials of the criminal case. Visualization of the originals significantly simplifies demonstration of technical details of electronic data, such as metadata, chronology, geolocation, digital identifiers and other numerical, temporal, navigation data on electronic maps.

12. Introduction of electronic document flow as a necessary condition for procedural and material saving, as a final significance of legalization of the electronic evidence notion. The use of the notions of electronic data and electronic evidences in legal systems of various states shows that paper (documentary) criminal case materials have become an anachronism and an atavism in the recent two decades. We believe that the use of the notions of electronic data and electronic evidences in the criminal-procedural legislation is of key significance for introducing the electronic document flow.

To implement the above provisions of the proposed concept, it is necessary to analyze the foreign criminal-procedural legislation.

3. Research of the electronic evidence in the legal systems of foreign countries

Inadmissibly slow changes in the Russian legislation and cardinal changes in foreign legal systems demonstrate the advantages of using electronic evidences in criminal-procedural legislations in terms of application, in particular, for introducing the electronic document flow.

[11] *Bank of Russia. Main directions of development of the financial market of the Russian Federation for 2022 and for the period of 2023 and 2024*. (2022). https://www.cbr.ru

The analysis of the notions of electronic evidence in the Anglo-Saxon legal system shows that digital evidences are defined as information and data valuable for investigation which are stored, received and transferred using an electronic device[12]. This said, the evidences obtained from electronic devices, such as computers and their peripherals, computer networks, mobile telephones, digital cameras, data storage devices, as well as from the Internet, are used in the proving process on the same legal bases as the traditional forms of evidences (Rogers et al., 2023; Reedy, 2023; Horsman, 2023). Legislative regulation of electronic evidences in Great Britain is stipulated by the Police and Criminal Evidence Act of 1984[13]. All digital evidences are regulated by the same rules and law as documentary evidences[14].

The authorities of the police stipulated in Article 19 of the Law on Police are expanded to vindication of any information, including in electronic form. The key condition is that electronic evidentiary information refers to commitment or prevention of crimes, and that its seizure facilitates prevention of concealment, loss, falsification or destruction of evidences in any form. Similar approaches to digital evidences are stipulated in the guide for British police[15].

Dictionaries of Anglo-Saxon law define digital evidence broadly – as information having evidentiary value, stored or transferred in digital form, i. e. any data recorded or stored on any carrier in a computer system or another similar device, which can be read or perceived by a human or a computer system[16]. Another law dictionary defines digital evidence or electronic evidence as any evidentiary information, stored or transferred in a digital form, while a party of a judicial dispute may use it during litigation[17].

Article 402 of the US Federal Rules of Evidence interprets digital evidence and both data and media storing the data[18]. The broad interpretation of the notion of evidences and using the notion of "data" in legislation has long enabled the United States to apply electronic document flow in criminal procedure. To implement this technology, guidelines

12 National Institute of Justice. (2008, April). *Electronic CSI, a Guide For First Responders, Electronic Crime Scene Investigation*: A Guide for First Responders, Second Edition (ojp.gov).

13 *Police and Criminal Evidence Act 1984*. (1984). https://www.legislation.gov.uk/

14 *Digitally Stored Evidence Standard Operating Procedure. Police Service of Scotland Standard Operating Procedure (SOP)*. (2018). https://www.scotland.police.uk/spa-media/ercbdgot/indecent-images-children-digital-media-sop.pdf

15 *ACPO Good Practice Guide for Digital Evidence*. (2012, March). https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

16 *Lawinsider*. 2021. https://www.lawinsider.org/

17 *US Legal Forms*. 2022. https://uslegal.com/wp-signup.php?new=www.definitions

18 *Federal Rules of Evidence*. (2020). federal_rules_of_evidence_-_december_2020_0.pdf (uscourts.gov)

were elaborated[19], as well as the guiding rules for courts of all levels and regulations for document presentation, technical requirements to electronic documents copying, scanning, to their format, volume, including using electronic automated databases[20]. Placement of criminal case materials in the information-technological environment grants the participants of a criminal procedure access to the criminal case materials for familiarization and notification. The published guidelines and practice of using the electronic document flow (Case Management and Electronic Case Files (CM/ECF) system)[21] attribute the key importance to a user account or personal page. The officials implementing the procedure, lawyers and applicants must create an account and automatically receive a generated password[22]. Abuse of one's account entails strict disciplinary and legal liability.

Introduction of the electronic document flow significantly simplifies the electronic registering and proceedings[23]. The elaborated guidelines stipulate requirements to the quality of electronic criminal-procedural documents and the distributed access of parties[24].

3.1. Notion of electronic evidence in the legislations of European states

In the continental system of law in the European Union, the extensive interpretation of electronic evidences as "any information, created, stored or transferred in a digital form, enabling to disavow a fact disputed during litigation"[25] demonstrates their most effective use in criminal procedures. In the era of digital technologies, the most intensive work over the introduction of electronic evidences in the EU countries began after the

19 *Electronic case filing administrative policies and procedures manual*. (2020, October). https://www.azd.uscourts.gov/sites/default/files/documents/adm%20manual.pdf

20 *Federal Rules of Evidence. R. 402. 2 Federal Rules of Evidence. R. 803*. (2020). https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_december_2020_0.pdf

21 *Electronic case filing administrative policies and procedures*. https://www.ncmd.uscourts.gov/sites/ncmd/files/ecfprocman.pdf

22 *Electronic case filing (ECF) Manuals and Training*. (2016). https://www.kywd.uscourts.gov/ecf-manuals-and-training

23 *SEC Center for Complaints and Enforcement Tips*. (2021). https://www.sec.gov/whistleblower/submit-a-tip

24 *Enforcement Manual*. (2017, November 28). https://www.sec.gov/divisions/enforce/enforcementmanual.pdf

25 *Electronic evidence guide. A basic guide for police officers, prosecutors and judges. Version 2.1, Strasbourg*. (2020, March). https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

European Parliament adopting Regulation providing cooperation mechanisms in 2018.[26] The extensive interpretation of electronic evidences and the adoption of the Regulation endowed the law enforcement and judicial bodies with contemporary tools for collecting evidences in electronic form, thus accelerating the process of their protection and obtaining from the subjects of information-technological systems, regardless of a country's jurisdiction (Horsman, 2023; Hoile et al., 2011; Mason, 2014).

Recognition of electronic data as criminal-procedural evidence in the EU countries facilitates interaction when investigating criminal cases in different countries. In order to develop legal assistance in criminal cases and operatively store the evidentiary information, the European Parliament adopted a Regulation stipulating mandatory European warrants for storing electronic data (European Preservation Order). According to the established procedure, an order is issued, which is confirmed by a judicial body of the requesting country. Non-submitting of the information requested entails strict administrative liability in the form of fines. Alongside with the orders on information preservation, the European Parliament adopted a European Production Order. The executors of the orders are holders of digital evidentiary information in information-technological networks, such as the Internet providers, communication providers, system administrators, and the so called providers of electronic communication services.

3.2. Notion of electronic evidence in the People's Republic of China

The information-technological potential created in the People's Republic of China (further – PRC) forms the basis for collecting electronic evidentiary information, providing a new information-technological regime or proving. Digital development in China cardinally changes the information-analytical and information-technological provision of crime investigation. The changes which occurred in China made it possible to transfer from documents to data, simultaneously simplifying the procedural form of criminal proceedings. The new approaches actually allowed eliminating the documentary (written) character of proceedings and transferring to an electronic format of a criminal case.

The epoch of electronic evidences started with the adoption of amendments to the Criminal-procedural Code of the People's Republic of China in 2012. Electronic data were added to the existing oral evidences: claims of victims, testimonies of witnesses, testimonies and explanations of suspects and defendants; material and written evidences; conclusions of experts; protocols of examination and survey; video- and audio materials[27].

---

[26] *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*. (2018). https://www.eclan.eu/en/eu-legislatory/proposal-for-a-regulation-of-the-european-parliament-and-of-the-council-on-european-production-and-preservation-orders-for-electronic-evidence-in-criminal-matters-e-evidence

[27] *Criminal-procedural Code of the People's Republic of China*. (2012). https://asia-business.ru/law/law1/criminal/procedurallaw/

Thus, since 2012, the Criminal-procedural Code of the People's Republic of China recognizes "electronic data" as evidences, although this notion is not explained in the criminal-procedural law (Yunshehn, 2014).

Developing the criminal-procedural law, PRC elaborated a joint Enactment "On solving certain issues related to collecting, receiving and analyzing electronic data in criminal cases", which stipulates the notion of electronic data. Article 1 of the said Enactment defines "electronic data" as information collected within the frameworks of a criminal case, preserved and transferred in electronic form, which may serve as evidence in a criminal case"[28].

Article 2 of the Enactment provides a classification of electronic data recognized as evidence in a criminal case, among which: websites, blogs (online diaries), microblogs, pages in social media, identifier applications (for example, WeChat), forums, online discs (online storages). Most significant are the communications in the Internet and communication networks, such as mobile messages, electronic mail, social media messages. Of utmost importance is identification information, obtained during user registration on websites, electronic transactions, from registers.

After the electronic evidences were included into the criminal-procedural legislation, some researchers optimistically marked that the era of electronic evidences would provide a historic improvement in the theory of evidences (Guo, 2023; Wu & Zheng, 2020; Chen et al., 2020).

To ensure the guarantees of integrity and consistency when collecting electronic evidences, Article 7 of the Enactment stipulates their withdrawal by two investigators simultaneously. The Enactment postulates strict observance of all the listed technical standards and legal requirements under the threat of their inadmissibility, stipulated in the criminal-procedural legislation.

During the withdrawal, the source data carrier is sealed and minutes of the state of storage of the source data carrier are produced. The sealing of the source data carrier and its photographing are to protect information from editing. If the source data carrier and the electronic data contained in it cannot be withdrawn, minutes are produced stating the reasons for impossibility to withdraw the source data carrier and the place of its storage. The electronic data located outside the PRC can be withdrawn via the Internet. After the criminal case investigation is finished, the source data carrier or the electronic data collected must be transferred with the case in a sealed form. Besides, reserve copies are transferred to the People's Prosecutor's Office and the court (Yuan, 2017).

[28] Enactment of the Supreme People's Court of PRC, Supreme People's Prosecutor's Office of PRC and Ministry of Public Safety of PRC. (2016). https://splcgk.court.gov.cn/gzfwww//spyw/spywDetails?id=84ba1d7cbc0540d59fe49341f8b1ef85

When electronic data are checked in the Prosecutor's Office and the court, the legality of their acquisition, their verity and relevance (actuality) should be analyzed.

In all jurisdictions, problems occur with storage of electronic data in the investigation bodies and transference of case materials to court. Globally, digital platforms are developed, databases are created, interdepartmental information networks are used. In this regard, PRC created an integrated database with online storage technology (similar to iCloud) to register, store and transfer criminal case materials in electronic form to court. The main functions of the cloud storage of the Chinese law enforcers are not only storing and archiving but also rapid search of the necessary materials in large massifs of electronic data. The developers of this information platform included the functions of surveillance over all stages of criminal-procedural activity, from monitoring the preliminary investigation to readjudication by superior authorities.

Thus, analysis of the Chinese criminal-procedural legislation as regards recognition of electronic data as evidences in PRC testifies to modernization of the criminal procedure in China.

3.3. Elaboration of international standards for electronic evidences

All international documents on cybercrime emphasize that digital data are the basis of most investigations and that effort is made towards further legal regulation. The European Convention on Cybercrime defines computer data as any presentation of facts, information or notions in the form suitable for processing in a computer system, including software capable of making a computer system execute a certain function (clause "b" of Article 1)[29].

The Convention defines "flow data" as any computer data referring to transmittance of information by a computer system, which are generated by a computer system being a constituent part of the relevant communication chain and indicate a source, purpose, route, time, date, size, duration or type of the respective network service (clause "e" of Article 1). The Convention uses the notion of "data" for operative provision and preserving, searching and withdrawal of the stored computer data. The most promising provisions are contained in Article 20 of the Convention, which stipulates online collection of data about information flows. In particular, states were charged with obligations to adopt legislative and other measures necessary to provide competent bodies with authorities to collect and record online, using technical means, the data about information flows and, within legal cooperation, to transfer the data to the party concerned.

[29] *Convention on Cybercrime (ETS no. 85)*. https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#OB9knUTgvfe6Gfbu1

International Criminal Police Organization, known as Interpol, is the organization facilitating police cooperation in member countries. The Interpol rules on information exchange define "data" as any information, regardless of its source, referring to the constituent elements of general criminal offenses, investigation and prevention of such offences, criminal prosecution of offenders and punishment for them[30]. The Interpol Guidelines for handling electronic evidences when executing search and withdrawal, their identification using methods guaranteeing their integrity, recommend handling them like any other traditional evidences. It should be taken into account that some electronic devices require special procedures of collecting, packing and transporting, either because they are subject to damage by electromagnetic fields or because their contents may change during handling and reserving[31].

The Russian Standard on information technologies, methods of providing safety, revealing and disclosing of electronic information introduces a new notion of "electronic discovery", serving as a driving force both when performing investigations and collecting and processing evidences[32]. Electronic discovery (e-discovery) is the process of revealing and presenting the relevant electronically stored information (ESI) or data by one or several parties participating in the investigation or litigation, or in similar procedures. As stipulated by the Standard, the constituent elements of e-discovery are collection, provision of preservation, presentation, and transfer of the information stored in electronic form. This is one of the modern standards based on earlier standards which also viewed evidences presented in digital form (digital evidence). This standard reads that the information or data stored or transferred as a binary code can be used as evidence[33].

Conclusions

Finalizing the research, we should mark that the authors' concept of electronic evidence is a system of information-technological and legal views on the criminal-procedural form, which is intended for optimizing the process of collecting, registering and preserving them in the criminal case materials. The main goal of the proposed concept consists

30 *Interpol's Rules on the Processing of Data*. (2021, March). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

31 *Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence*. (2021). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

32 *GOST R ISO/MEC 27050-1-2019 Information technologies. Methods of safety provision. Identification and disclosure of electronic information. Part 1. Review and concepts*. (2019). Moscow: Standartinform.

33 *ISO/IEC 27037:2014 "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence"*. (2014).

in modernizing the criminal-procedural proving while revealing the potential of electronic evidences in the said directions.

Implementation of the proposed concept will facilitate a breakthrough in the archaic system of evidentiary law and move beyond the written (paper) form of registering evidences. The first step to implementing the said concept should be inclusion of the "electronic evidence" notion into the Criminal-procedural Code; this will entail the unobstructed use of electronic evidentiary information by investigation agencies and courts and using it as a means of proving. An essential element of the proposed concept is separation of electronic information from the documentary (paper) investigation protocol and electronic carrier of information with the prospect of forming an electronic workflow on an interdepartmental digital platform.

We propose to consider the notion of electronic evidences, earlier proposed by the authors in the context of elaborating new approaches to information provision of criminal-procedural activity, within the frameworks of a broader concept and to include it into Article 5 of the Criminal-procedural Code in the following edition: "…electronic evidence is juridically significant information registered by electronic means or presented in electronic form, in compliance with the criminal-procedural requirements applied to evidences with a view of establishing the truth in a criminal case" (Pastukhov, 2022a).

Alongside with introducing the notion of electronic evidences, Article 84 of the Criminal-procedural Code should include the notion of electronic data, with a view of breaking the obsolete system of documentary "other documents".

Under the information society, well-developed digital infrastructure, inclusion of these notions will create the information-technological regime of proving based on scientific organization of labor. Practically speaking, it will enable to ensure, in a new way, the informational advantage of investigation agencies and courts against criminal activity in terms of collecting and registering of electronic evidentiary information. In terms of interaction of the preliminary investigation bodies with any subjects of information-technological systems it will significantly reduce the temporal, procedural and material costs through electronic workflow. Inclusion of this notion will allow the officials to not only collect and store evidentiary information in electronic form without its linking and transferring on an electronic carrier of information, but also register the traditional analog evidentiary information electronically, using computer, audio-, and video means of recording.

References

Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of block-chain in electronic evidence generation. *Forensic Science International: Digital Investigation*, *35*, 301001. https://doi.org/10.1016/j.fsidi.2020.301001

de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, *34*(2), 327–336. https://doi.org/10.1016/j.clsr.2018.01.003

Golovko, L. V. (2019). The digitalization in criminal procedure: local optimization or global revolution? *Vestnik ekonomicheskoi bezopasnosti*, *1*, 15–25. (In Russ.). https://doi.org/10.24411/2414-3995-2019-10002

Golubtsov, V. G. (2019). Theory of evidence and digitization in civil proceedings. *Perm Legal Almanac*, *1*, 379–387. (In Russ.).

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, *209*(1–3), 143–148. https://doi.org/10.1016/j.forsciint.2011.01.017

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, *63*(1), 116–126. https://doi.org/10.1016/j.scijus.2022.11.004

Lippman, M. R. (2019). *Criminal Procedure*. Sage.

Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, *30*(1), 80–84. https://doi.org/10.1016/j.clsr.2013.12.005

Pastukhov, P. S. (2019). Electronic evidence in the regulatory system of criminal procedural evidence. *Perm Legal Almanac*, *2*, 695–707. (In Russ.).

Pastukhov, P. S. (2022a). New approaches to information provision of criminal-procedural activity. In T. V. Evtukh, L. Yu. Mkhitaryan et al. (Ed. board), A. N. Samoilov (xec. ed.), S. A. Kotova (in charge of the issue), *State and municipal governance in Russia: condition, problems and prospects: works of the All-Russia scientific-practical conference, Perm, November 17, 2022* (pp. 139–143). Perm: Perm. filial RANKhIGS. (In Russ.).

Pastukhov, P. S. (2022b). Digital identification of a personality. In T. P. Podshivalov, E. V. Titova, E. A. Gromova (Eds.), *Digital environment law* (pp. 625–632). Moscow: Prospekt. (In Russ.).

Reedy, P. (2023). Digital Evidence: Overview. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). https://doi.org/10.1016/b978-0-12-823677-2.00268-3

Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). https://doi.org/10.1016/b978-0-12-823677-2.00029-5

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Voronin, M. I. (2019). Electronic Evidence in the Criminal Procedure Code: To Be or not to Be? *Lex russica*, *7*, 74–84. (In Russ.). https://doi.org/10.17803/1729-5920.2019.152.7.074-084

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review, 36*, 105401. https://doi.org/10.1016/j.clsr.2020.105401

Yuan, Yi. (2017). Study on judge's capacity on evidence review from the perspective of the revised criminal procedure law of China. *Sociopolitical Sciences*, *3*, 137–138. (In Russ.).

Yunshehn, Ch. (2014). Legislative rules of using electronic data on the results of search and arrest. *Sovremennoe Pravo*, *36*(5), 111–113. (In Russ.).

Zaytsev, O. A., & Pastukhov, P. S. (2019). Formation of a New Strategy for Crime Investigation in the Era of Digital Transformation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, *46*, 752–777. (In Russ.). https://doi.org/10.17072/1995-4190-2019-46-752-775

Zaytsev, O. A., & Pastukhov, P. S. (2022). Digital personal profile as an element of the information and technological strategy of crime investigation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, *56*, 281–308. (In Russ.). https://doi.org/10.17072/1995-4190-2022-56-281-309

Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, *155*, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138

Zuev, S. V., & Sutyagin, K. I. (2016). *Criminal procedure*: tutorial. Chelyabinsk: Izdatel'skii tsentr YUURGU. (In Russ.).

Authors information

Anna A. Dmitrieva – Doctor of Law, Associate Professor, Head of the Department of Criminal and Penal Law and Criminology, South Ural State University (National Research University)
Address: 76 prospekt Lenina, 454080 Chelyabinsk, Russian Federation
E-mail: annadm@bk.ru
ORCID ID: https://orcid.org/0000-0002-1035-1387
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/GWU-5850-2022
Scopus Author ID:
https://www.scopus.com/authid/detail.uri?authorId=57281194100
Google Scholar ID: https://scholar.google.com/citations?user=B0PWOwEAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=312402

Pavel S. Pastukhov – Doctor of Law, Associate Professor, Professor of the Department of Criminal Procedure and Criminology, Perm State National Research University; Professor of the Department of Public Law, Perm Institute of the Federal Penitentiary Service
Address: 15 Bukirev Str., 614990 Perm, Russian Federation; 125 Karpinskiy Str., 614012 Perm, Russian Federation
E-mail: pps64@mail.ru
ORCID ID: https://orcid.org/0000-0003-0391-5540
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/B-5451-2017
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56926673600
Google Scholar ID: https://scholar.google.com/citations?user=fu844_kAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=405105

Authors' contributions

Substantiation of the research concept; comparative analysis; summarization of the research results; wording of conclusions; interpretation of the research results were carried out by A. A. Dmitrieva and P. S. Pastukhov in equal parts.

Conflict of interests

The authors declare no conflict of interests.

Funding

The research was not sponsored.

Article history

Date of receipt – January 5, 2023
Date of approval – February 5, 2023
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023

Научная статья
УДК 343.1:168.3:004.91
EDN: https://elibrary.ru/sgaoks
DOI: https://doi.org/10.21202/jdtl.2023.11

Концепция электронного доказательства в уголовном судопроизводстве

Анна Александровна Дмитриева ✉

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Павел Сысоевич Пастухов

Пермский государственный национальный исследовательский университет
г. Пермь, Российская Федерация
Пермский институт Федеральной службы исполнения наказаний
г. Пермь, Российская Федерация

Ключевые слова

Информация,
право,
процесс доказывания,
расследование,
суд,
уголовное дело,
уголовный процесс,
цифровые технологии,
электронное взаимодействие,
электронные доказательства

Аннотация

Цель: раскрытие потенциала цифровой трансформации для выработки оптимальных средств и методов собирания доказательств, внедрения научной организации труда должностных лиц, осуществляющих уголовное судопроизводство. Научный подход концепции состоит в минимизации затрат на собирание доказательственной информации по уголовным делам в электронной форме и электронным способом, а также сохранении материалов уголовного дела в электронной форме.

Методы: ведущее место среди методов исследования занимает диалектический метод, в соответствии с которым проблема электронного документа рассматривается во взаимосвязи и взаимозависимости с информационно-технологическим развитием общества. Совокупность методов научного познания в исследовании создает предпосылки для объективного и комплексного подхода к выделенным проблемам.

Результаты: авторская концепция электронного доказательства представляет собой систему информационно-технологических и правовых взглядов на уголовно-процессуальную форму, призванную оптимизировать процесс их собирания, фиксации и сохранения в материалах уголовного дела. Развитие концепции нацелено на выработку новых подходов к организации деятельности органов расследования и суда с учетом достижений в сфере информационных технологий, обеспечивающих новые способы собирания уголовно-релевантной,

✉ Контактное лицо

уголовно-процессуальной, криминалистически значимой информации при расследовании и рассмотрении уголовного дела. Представленная концепция направлена также на совершенствование взаимодействия и служебной коммуникации должностных лиц органов предварительного расследования с должностными лицами информационно-технологических систем для собирания доказательственной информации в электронной форме.

Научная новизна: системно проанализированы изменения, происходящие в современном информационном обществе через призму возникающих проблем между отраслевым уголовно-процессуальным доказательственным правом и более современными технологическими способами собирания доказательственной информации. В статье демонстрируется новый подход к созданию технологического взаимодействия с использованием цифровых технологий на научной основе организации доказательственной деятельности, призванной оптимизировать и рационализировать процесс доказывания в уголовном судопроизводстве.

Практическая значимость: материалы исследования могут быть использованы в работе по подготовке предложений о внесении изменений и дополнений в действующее законодательство с целью реализации практического опыта уже действующих моделей уголовно-процессуальной деятельности зарубежных стран, неисчерпаемого потенциала информационных технологий, программного обеспечения, искусственного интеллекта для рационализации доказывания по уголовным делам.

Для цитирования

Дмитриева, А. А., Пастухов, П. С. (2023). Концепция электронного доказательства в уголовном судопроизводстве. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Список литературы

Воронин, М. И. (2019). Электронные доказательства в УПК: быть или не быть? *Lex russica*, *7*, 74–84 EDN: https://elibrary.ru/jzbdut. DOI: https://doi.org/10.17803/1729-5920.2019.152.7.074-084

Головко, Л. В. (2019). Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? *Вестник экономической безопасности*, *1*, 15–25. EDN: https://elibrary.ru/korqgw. DOI: https://doi.org/10.24411/2414-3995-2019-10002

Голубцов, В. Г. (2019). Теория доказательств и цифровизация в гражданском судопроизводстве. *Пермский юридический альманах. Ежегодный научный журнал*, *1*, 379–387. https://elibrary.ru/zywect

Зайцев, О. А., Пастухов, П. С. (2019). Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации. *Вестник Пермского университета. Юридические науки*, *46*, 752–777. https://doi.org/10.17072/1995-4190-2019-46-752-775

Зайцев, О. А., Пастухов, П. С. (2022). Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений. *Вестник Пермского университета. Юридические науки, 56*, 281–308. https://doi.org/10.17072/1995-4190-2022-56-281-309

Зуев, С. В., Сутягин, К. И. (2016). *Уголовный процесс*: учебник. Челябинск: Издательский центр ЮУрГУ.

Пастухов, П. С. (2019). Электронные доказательства в нормативной системе уголовно-процессуальных доказательств. *Пермский юридический альманах*, *2*, 695–707. https://elibrary.ru/htypyz

Пастухов, П. С. (2022a). Новые подходы к информационному обеспечению уголовно-процессуальной деятельности. В сб. Т. В. Евтух, Л. Ю. Мхитарян и др. (ред. кол.), А. Н. Самойлов (отв. ред.), С. А. Котова (отв. за вып.), *Государственное и муниципальное управление в России: состояние, проблемы и перспективы: материалы Всерос. науч.-практ. конф., г. Пермь, 17 ноября 2022 г.* (с. 139–143). Пермь: Перм. филиал РАНХиГС.

Пастухов, П. С. (2022b). Цифровая идентификация личности. В книге: Т. П. Подшивалов, Е. В. Титова, Е. А. Громова (ред.). *Право цифровой среды*: монография (с. 625–632). Москва: Проспект. https://elibrary.ru/zomcik

Юань, И. (2017). Проблемы рассмотрения доказательств по новому УПК КНР. *Социально-политические науки*, *3*, 137–138.

Юншэн, Ч. (2014). Законодательные правила использования электронных данных результатов обыска и ареста. *Современное право*, *36*(5), 111–113.

Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Science International: Digital Investigation*, *35*, 301001. https://doi.org/10.1016/j.fsidi.2020.301001

de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, *34*(2), 327–336. https://doi.org/10.1016/j.clsr.2018.01.003

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, *209*(1–3), 143–148. https://doi.org/10.1016/j.forsciint.2011.01.017

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, *63*(1), 116–126. https://doi.org/10.1016/j.scijus.2022.11.004

Lippman, M. R. (2019). *Criminal Procedure*. Sage.

Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, *30*(1), 80–84. https://doi.org/10.1016/j.clsr.2013.12.005

Reedy, P. (2023). Digital Evidence: Overview. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). https://doi.org/10.1016/b978-0-12-823677-2.00268-3

Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). https://doi.org/10.1016/b978-0-12-823677-2.00029-5

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review, 36*, 105401. https://doi.org/10.1016/j.clsr.2020.105401

Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, *155*, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138

Сведения об авторах

Дмитриева Анна Александровна – доктор юридических наук, доцент, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Российская Федерация, г. Челябинск, проспект Ленина, 76
E-mail: annadm@bk.ru
ORCID ID: https://orcid.org/0000-0002-1035-1387
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/GWU-5850-2022
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57281194100
Google Scholar ID: https://scholar.google.com/citations?user=B0PWOwEAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=312402

Пастухов Павел Сысоевич – доктор юридических наук, доцент, профессор кафедры уголовного процесса и криминалистики, Пермский государственный национальный исследовательский университет; профессор кафедры публичного права, Пермский институт Федеральной службы исполнения наказаний
Адрес: 614990, Российская Федерация, г. Пермь, ул. Букирева, д. 15;
614012, Российская Федерация, г. Пермь, ул. Карпинского, д. 125
E-mail: pps64@mail.ru
ORCID ID: https://orcid.org/0000-0003-0391-5540
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/B-5451-2017
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56926673600
Google Scholar ID: https://scholar.google.com/citations?user=fu844_kAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=405105

Вклад авторов

Обоснование концепции исследования; проведение сравнительного анализа; обобщение результатов исследования; формулировка выводов; интерпретация результатов исследования осуществлялись А. А. Дмитриевой и П. С. Пастуховым в равных долях.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 5 января 2023 г.
Дата одобрения после рецензирования – 5 февраля 2023 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн-размещения – 10 марта 2023 г.