PROVIDING ELECTRONIC INTERNET EVIDENCE IN RUSSIAN NOTARIAL AND JUDICIAL PRACTICE FOR CIVIL LAW DISPUTES

PROPORCIONAR EVIDENCIA ELECTRÓNICA DE INTERNET EN LA PRÁCTICA NOTARIAL Y JUDICIAL RUSA PARA DISPUTAS DE DERECHO CIVIL

Artur G. Kravchenko[1]*; Aleksey I. Ovchinnikov[2]; Andrey A. Romanov[3]; Tatiana Yu. Kareva[4].

1. Far Eastern Federal University, Russia. kravchenko_artur@mail.ru
2. South Federal University, Russia. k_fp3@mail.ru
3. Far Eastern Federal University, Russia. romanov.aal@dvfu.ru
4. Far Eastern Federal University, Russia. kareva.tyu@dvfu.ru

*corresponding author: Artur G. Kravchenko email: kravchenko_artur@mail.ru

ABSTRACT

The current study is mainly devoted to the analysis of the current Russian legislation and the emerging notarial and judicial practice in the field of providing electronic evidence, the features and problems of procedures for their notarization, the relevance and admissibility of electronic evidence in civil law disputes in courts of general jurisdiction and arbitration courts as a factor in stabilizing civil law turnover carried out in information and communication formats (digital economy). Moreover, the study considers the problems of legal recording electronic traces while noting the most significant aspects of this recording of the evidence and formulating recommendations for notaries and parties to judicial disputes. To that aim, a range of general scientific methods, including observational, descriptive, and qualitative approaches, are used. Based on the results, the Russian regulatory system must have mechanisms for fixing traces of such civil activity to use them as evidence in civil and arbitration disputes.

Keywords: securing evidence; digital traces; digital documents; notary public; notarial services.

Revista de Investigaciones Universidad del Quindío,
34(S3), 232-243; 2022.
ISSN: 1794-631X e-ISSN: 2500-5782

RESUMEN

El estudio actual está dedicado principalmente al análisis de la legislación rusa actual y la práctica notarial y judicial emergente en el campo de la provisión de evidencia electrónica, las características y problemas de los procedimientos para su certificación notarial, la relevancia y admisibilidad de la evidencia electrónica en disputas de derecho civil. en tribunales de jurisdicción general y tribunales de arbitraje como factor de estabilización de la rotación de derecho civil realizada en formatos de información y comunicación (economía digital). Además, el estudio considera los problemas del registro legal de las huellas electrónicas al mismo tiempo que señala los aspectos más significativos de este registro de la prueba y formula recomendaciones para los notarios y las partes en los litigios judiciales. Con ese fin, se utiliza una variedad de métodos científicos generales, que incluyen enfoques observacionales, descriptivos y cualitativos. Con base en los resultados, el sistema regulatorio ruso debe tener mecanismos para fijar rastros de dicha actividad civil para usarlos como evidencia en disputas civiles y de arbitraje.

Palabras clave: aseguramiento de prueba; huellas digitales; documentos digitales; notario público; servicios notariales.

INTRODUCTION

In 2020, the legislator largely implemented the concept of electronic notaries by introducing a fairly large body of legislation regulating the relevant procedure for the provision of notarial services (Orders of the Ministry of Justice of Russia, which will determine the implementation of the "digital notariate", are registered). One of the elements for the development of electronic notariate was the changes concerning the provision of electronic evidence on the information and communication Internet network (Kashanin & Churakov, 2021).

According to article 71 of the Civil Procedure Code of the Russian Federation, article 75 of the Arbitration Procedure Code of the Russian Federation and article 70 of the Administrative Procedure Code of the Russian Federation, "written evidence is evidence containing information about the circumstances that are important for the consideration and resolution of the case, acts, contracts, certificates, business correspondence, other documents and materials made in the form of a digital or graphic record, including those obtained by facsimile, electronic or other communication, using the information and telecommunications Internet network, via a videoconference channel (if there is a technical possibility for such transfer of documents and materials), documents signed with an digital signature in the manner prescribed by the legislation of the Russian Federation, or executed in another way that allows establishing the authenticity of the document" (Golubeva & Drogoziuk, 2019). At the same time, electronic traces are an extremely complex element for the methodology of proving in all kinds of judicial proceedings; this is due to the special properties of electronic evidence, which must be taken into account in the practical work of a lawyer (Goncharova et al., 2019). Obviously, the special properties of digital evidence bring certain procedural problems to legal practice; the solution of those problems is reflected in many scientific publications. In particular, the publication Electronic evidence in civil and administrative proceedings (Guidelines and explanatory memorandum), 2020, notes that "if a court asks a party to submit printouts of electronic evidence, such party should not be prevented from providing the relevant metadata (Yakupov et al., 2020).

Place among written evidence; their growing role is due to the rapid development of information and communication technologies in all branches of law, including private legal relations. The institute of securing evidence in private law disputes is designed to help stabilize, predict and guarantee compliance with the principle of justice, good faith of the parties to civil-law turnover in a dynamic digital economy. The vector set by the Supreme Court of the Russian Federation on the strict observance of the ideas on good faith and proper conduct of participants in civil-law relations also confirms the above circumstances (Smirenskaya et al., 2019).

METHODS

To meet the aim of the study, a range of general scientific methods, such as observational, descriptive, and qualitative approaches are taken into account. The normative-legal acts of the current legislation of the Russian Federation, as well as examples of judicial and generalized notarial practice are used within the framework of the present research. The scientific paper is also based on expert and scientific views, developments on the problems of law enforcement of the current legislation on notariate and comprehension of the prospects concerning legislative development of "electronic notariate" as an integral part of the Russian legal policy to ensure the institutional development of national and international digital economy.

In the paper, the authors have outlined positions on the development of legal regulation of notarial activity in the digital environment as an unconditional and obligatory condition for the uniform efficiency of the e-commerce chain, including those parts in which notarial acts are involved: certification of remote transactions, recording the digital evidence of transactions, and legally significant actions in the information and communication Internet network.

The methodological complexity of building new legal constructions regulating the order of notarial and judicial actions in relation to the digital environment of the Internet lies in the fact that the previously existing theoretical-methodological and conceptual developments of legal regulation in the physical world record patterns of social relations different from the digital environment. Technocratic nature of the digital form of social relations, and their specificity in details require a revision of existing legal algorithms. Now the legislator needs to take into account the technical nuances that significantly affect the legal relations and the process of proving the circumstances of a particular legal dispute (Polina-Stashevskaya, 2022). In turn, the attempt to implement classical approaches to the electronic specifics of social relations leads to the unreliability or irrelevance of digital evidence in the process of proving. The very essence of electronic evidence introduces its own peculiarity and requires specific technical guarantees to be legally fixed (Rusakova et al., 2020).

RESULTS AND DISCUSSION

The technical complexity of ensuring the reliability of electronic evidence in court proceedings forms the need for a special approach to their legal fixation (Kashanin & Churakov, 2021). Thus, the need to record legally significant digital information located on the Internet most often arises in the following cases related to the need to protect the rights of subjects of economic and civil turnover:

- Publications discrediting the honour, good name and business reputation of the applicant;
- Unfair advertising that violates the applicant's rights to fair competition;
- Use of information (objects of intellectual property rights), or providing access to this information

that violates the intellectual rights of the applicant (author, right holder);
- Assignment of a domain name belonging to the applicant;
- Exchange of electronic messages and documents testifying to the conclusion of the transaction by the applicant or his/her legal representative;
- Validity of the contested restriction of applicant's access to his/her account, or the misappropriation of the account by a third party;
- Misuse of the applicant's personal data.

Note that notarization of electronic evidence occurs when there is reason to believe that (Rusakova & Frolova, 2019):

1. The rights of the applicant are violated or will be violated
2. A dispute arises in civil, arbitration or administrative proceedings
3. Presentation of evidence will become impossible or difficult in a judicial or administrative case

A Notary has no authority to secure evidence in criminal proceedings. However the circumstances notified by the Notary (as information about facts) can be implemented through prejudice, i.e. court determination of other circumstances not subject to further proving and reflected in a judicial act pronounced on the case within the framework of civil, arbitration or administrative proceedings (Golubeva & Drogoziuk, 2019).

Thus, notarial securing of evidence is a person's right to preventive measures of legal protection when a legal conflict may arise.

The grounds for application made by interested persons to a Notary Public for securing evidence are governed by Article 102 of the Fundamental Principles of Legislation of the Russian Federation on the Notariate. Such addressing was previously possible in the absence of an ongoing judicial or administrative review of the case. However, since January 1, 2015 the part 2 has lost its force (Rusakova et al., 2020), and currently there are no such restrictions on securing evidence, the courts accept notarized evidence, including electronic one, and evidence executed during a court case.

As a general rule, a Notary shall notify the parties and interested persons of the time and place of securing evidence (Nakhova, 2022). However, electronic evidence located both in the global and local networks does not fall under this rule for a number of reasons. Thus, exceptions to the above-mentioned rule are allowed in cases of urgency or when it is impossible to determine who will subsequently participate in the case. Notary practice defines the risk of loss of evidence as a non-precedential reason, which is an evaluative category. Meanwhile, legally relevant information stored on the servers of the Internet, including information from websites, messengers (WhatsApp, Telegram, etc.), mailboxes, social networks (VKontakte, Odnoklassniki, etc.), as well as stored on trading digital platforms (Aliexpress, Farpost, Avito, etc.), can be lost or edited both by the owners of these information resources and by third parties admitted to their moderation, as well as through unauthorized access. Thus, with regard to electronic traces in the Information and Communication Internet network, such risks of loss are indisputable in all cases, which is confirmed by the position of the Federal Chamber of Notaries, see para. 2 of the Letter from the Federal Chamber of Notaries dated 13.01.2012 No. 12/06-12 "On securing the notary with the evidence" (Polina-Stashevskaya, 2022).

Since 2019, according to article 103 "Fundamental Principles of Legislation of the Russian Federation on the Notariate" (approved by the Supreme Court of the Russian Federation on 11.02.1993 No. 4462-1) (wording of 30.12.2020) Notaries are authorized to provide evidence in the form of inspection of information located in the information and telecommunication Internet network remotely. This power has gained the greatest significance during the period of restrictive measures in connection with Covid-19, as well as in other life situations that do not allow the applicant to be personally present at a Notary.

The provision of evidence (electronic traces) according to clause 44.3 of the Fundamental Principles of Legislation of the Russian Federation on the Notariate can also be remotely carried out only by identifying the applicant by means of checking him/her with his/her enhanced digital signature with which the application in the established form is certified by the means of the notary's unified information system. The application itself is sent by the applicant to the Notary through the web-resource of the Federal Chamber of Notaries or the Unified Portal of State and Municipal Services (Functions) (Smirenskaya et al., 2019).

However, it should be noted that digital signatures do not guarantee 100% identification of a person either, as the monopoly right for digital signature keys can be lost either by the user himself/herself or be abused by the certification centre. However, the Notary verifies the formal authenticity of an enhanced digital signature, not the validity of its use by the proper person.

In furtherance of the electronic notariate concept, in the remote application of the applicant in accordance with Article 42 of the " Fundamental Principles of the Legislation of the Russian Federation Concerning Notarial Services" (approved by the Supreme Court of the Russian Federation No. 4462-1 dated 11.02.1993), now it is possible to identify a person through the provision of applicants' cell phone number to check his/her identity by face and voice (biometric data) through a Unified Information System of Notaries (Goncharova et al., 2019).

The interest of the applicant for notarization of evidence is determined by procedural norms provided by article 61 of the Civil procedural code of the Russian Federation and article 69 of the Arbitration procedural code of the Russian Federation which exempt the parties from proving the circumstances, if they are notarized, on condition of authenticity of notarized document and absence of essential violations in the order of a notarial action. That is, the procedural law establishes the presumption of reliability of notarized evidence.

When securing evidence, a notary does not decide the issue of relevance and admissibility of evidence, because this is the competence of the court or administrative body considering a case (Kashanin & Churakov, 2021). In this case, the case of a notary is to record and secure evidence, while the assessment of evidence is the exclusive prerogative of a court, including on the issue of its relevance and admissibility.

It should be especially noted that in accordance with clause 7 of the Resolution of the plenary meeting of the Supreme Court of the Russian Federation No.16 On Practice of Application by the Courts of the Law of the Russian Federation "On Mass Media" dated 15 June 2010, federal laws do not provide for any restrictions on the means of proving the fact of dissemination of information via telecommunications networks (including via Internet sites). Therefore, in resolving the question of whether such a fact occurred, the court, by virtue of Articles 55 and 60 of Civil Procedure Code of

the Russian Federation, has the right to adopt any means of proof provided for by civil procedural legislation. This position is held by the cassation instance of the arbitration court system in the field of intellectual property disputes represented by the Court for Intellectual Rights, which in case No. A40-239086/2016 pointed out that persons involved in the case may independently record information on the Internet by means available to them, including without resorting to the assistance of Notary.

Moreover, modern software can record (automatically form an analogue of) a technically detailed Notarial Inspection Protocol, using such service as the ShotApp.

It follows that the common method of notarizing electronic evidence by simply copying http link from the address bar of the browser, including it in the protocol and attaching a screenshot, and video recording of the site inspection becomes uninteresting to applicants, especially because of the high cost of the service, as well as the use of alternative methods of proof.

In this regard, in our opinion, the notarization of electronic evidence located on the Internet should still meet the requirements of technical and legal validation by the notary, which greatly complicates the notary's work, but makes the costs incurred by the applicant justified.

In other words, despite the position expressed by the Court of Intellectual Rights on the possibility of persons involved in the case to independently record the information they need on the Internet, nevertheless, the lack of notarization of such fixation causes the objection of the other party to the possibility of using such means of proof justifiable. The fact is that the parties, being in a legal conflict, tend to distrust each other and treat with mutual mistrust the documents and evidence provided in the case by the opposite party or by third parties. In view of the concerns previously raised that online information can be modified or deleted without any significant difficulty, the role of the notary as an independent entity that impartially and unbiasedly confirms the existence and content of certain information on the Internet becomes particularly important.

In order for the Notary to compile an Internet site inspection protocol that meets the requirements of technical authenticity of evidence, it is necessary to understand the methodological basics of electronic evidence fixation. Thus, the role and significance of electronic traces notarization is determined by the level of digital and legal competence of the Notary and the persons the Notary involves in the process of recording this type of evidence.

The definition of Internet is a rather broad notion that includes various types of information digital communications with their own trace specifics: web-sites, messengers, social networks, video hostings, electronic databases, file exchanges, postal services, aggregators, electronic exchanges, etc. All the above resources are means of information exchange and may become the subject of notary's research in order to provide demanded evidence, as evidenced by the emerging judicial practice in civil and arbitration cases.

First of all we'd like to mention that on the basis of article 103 of "Fundamental Principles of the Legislation of the Russian Federation Concerning Notarial Services" (approved by the Supreme Court of the Russian Federation on 11.02.1993 No. 4462-1) (wording of 30.12.2020) securing electronic evidence (if the information is on the Internet and there are risks of its destruction or distortion) is performed by the Notary without informing one of the parties and interested parties. Also, such notification is not carried out when it is impossible to determine who will subsequently participate in

the case. At the same time, it should be noted that processing of personal data of both the applicant and the persons whose personal data is necessary to process for the recording of evidence the Notary has the right to do so without their special consent (Rusakova & Frolova, 2019). The processing of personal data is vital to identify the parties, without which the courts will not recognize the electronic evidence as authentic.

Notaries face a number of typical risks when examining digital evidence and logging it:

1. There is a risk of domain name spoofing when researching web sites.
2. When inspecting mail servers, mail accounts can be spoofed and mail correspondence can be tampered with.
3. The possibility of falsification of accounts, correspondence in messengers, social networks is allowed.
4. There is an insufficient amount of information recorded by a notary for proof.
5. There is subjective uncertainty (affiliation) of the participants of electronic messages, etc.

Of course, it is technically impossible for a Notary Public to ensure the absolute reliability of electronic evidence located on the Internet. The Notary certifies a fact, not examines the evidence, and does not give it a legal assessment. On the other hand, a proper understanding of technical complexity of providing a particular electronic trace, involvement of necessary specialists (experts) in this process (Blanchette, 2012; Voznesenskaya, 2022), as well as general digital literacy, determination of sufficiency of recorded information significantly reduces the risks of logging unreliable or incomplete evidence.

Focusing on specific problems and features of fixation of digital traces of legally significant information, it seems necessary to highlight the following.

Thus, when inspecting sites, it is necessary to pay attention to known tricks of substitution of official domain names. In particular, the browser search bar containing a link to the Internet source: "//http", etc. can contain substituted domain names. For example, Sberbank.ru and Sberbnk.ru. Domain name substitution can be carried out through a different alphabet, which visually does not differ from the official one. To solve this technical problem, special software is used that allows generating an inspection protocol for the site according to the established methodology. For example, it is the program ARM Notary, with the site inspection module connected.

Another aspect of the examination of web pages is the notarization of the transcript of the HTML-code of the site, which may contain an infringement of intellectual rights. The applicant (right holder) may be interested in fixing the fact that the infringer used its trade name or commercial designation or trademark within the HTML code of the website. Typically, their use with HTML code is carried out in order to artificially promote their own site due to the popularity of the corresponding objects of intellectual property rights. An increasing number of arbitration disputes in this category only confirms this fact.

Critically important here is the determination of the location of objects that infringe intellectual property rights, because the structure of the organization of sites allows the creation of an allusion of placing a particular web-resource, although, in fact, for example, a disputed object of intellectual rights can be loaded by the site from another web-resource, including automatic performance of this action. Therefore, the notarization of a web-page by means of a simple PrintScreen as evidence

(Nakhova, 2022) may be questioned by the court, and it is also possible that it may be rejected, despite the recognition of the screenshot as admissible evidence (Goncharova et al., 2019). For example, the Arbitration Court of Moscow on December 24, 2010 for the Case No. A40-94778/2010 in the operative part of its decision has noted that "from the notarial record it follows that the disputed photos are available on the Internet, but the inspection does not identify whose server hosted the disputed photos, respectively, it is impossible to conclude who exactly makes the picture to the public.

The specifics of site browsing also require special knowledge and other features of structuring web resources (sites). So, geotargeting changes the content of sites depending on what region is being viewed from. For example, the range of goods, the price of goods, and its availability on the site generates information for a particular city, region, etc. The structure of some sites changes dynamically depending on the conditions set by the owner of the web resource.

Resource domain names can be linked to their owner only for a limited time, which requires a technical verification of the belonging of the site to the appropriate owner at the time of filing the protocol (Tokarev et al., 2019).

It should be noted that in addition to the correct fixation of information about the site itself, it is important to record the information posted on it. So, for example, the plaintiff was able to defend his legitimate interests under the exclusive right thanks to detailed recording in the protocol of the object of intellectual rights (photo). The Ruling of the Judicial board on civil cases of the Supreme Court of the Russian Federation dated 28.01.2020 No. 5-KG19-228, 2-3052/2018, when considering the case of banning the use of photographic work, recovery of compensation for violating the exclusive right to work, and compensation for moral damage noted that the protocol of the inspection of the website and the photo posted on it, certified by a notary, was accompanied by the original digital file photo, data on the serial number of the camera, which took a photograph. This circumstance was decisive in proving the authorship of the photo posted in the public domain, but used by the defendant for commercial purposes.

It is also important to check the availability of the disputed information on the site, which must be indicated by the applicant. Thus, when reviewing the acts of lower courts in the case of protection of business reputation in cassation proceedings, the Ruling of the Supreme Court of the Russian Federation dated 12.11.2020 No. 307-ES20-17437 in case No. A56-49075/2018 established that when considering this case the courts, having studied the evidence submitted by the parties, and being guided by the rules of the Civil Code of the Russian Federation and the explanations contained in the Resolution of the Plenum of the Supreme Court of the Russian Federation dated 24.02.2005 No. 3 "On judicial practice in cases involving the protection of honour and dignity of citizens, as well as the business reputation of citizens and legal entities" (hereinafter - the Decision N 3), found that in confirmation of the fact of dissemination of the disputed information, the plaintiff presented protocols drawn up by the notary of of inspection of the website www.sunpeterburg.ru and inspection of the e-mail. However, there is no information about the placement of the disputed article on the website www.sunpeterburg.ru in the website inspection protocol presented by the plaintiff. In turn, personal correspondence by email cannot be assessed as an attack on honour and good name, because it is not in the public domain (Tarakanov et al., 2019).

Finally, it is thought that it is necessary to temporarily record not only the moment of fixation of evidence, but also the placement of disputed information on the site under investigation. For example,

in the Decision of the Court of Intellectual Rights No. C01-706/2018 dated 21.09.2018 in case No. A56-58839/2017 it is noted that "the evidence indicating that the disputed audiovisual work was placed on the Internet beyond the period of authorized use, was not presented in the case file, while the notarial protocols of inspection of evidence available in the case file certify only the fact of the presence of these videos in the Internet at the date of its making and contain no information about the date of their placement, which was reasonably taken into account by the court. Thus, the Notary's mistake of failing to record the date of posting of the disputed information led to the rejection of the relevant evidence and a different procedural outcome of the resolution of the case on the merits (Voznesenskaya, 2022).

As messengers are increasingly integrated into business communication, they are increasingly used not only for personal communication, but also for corporate communication, as well as in the exchange of information on transactions, etc., their examination as part of the provision of evidence is also significantly widespread. But unlike websites, messengers have their own specifics, which should be taken into account in a notarial inspection protocol.

Thus, it is important to identify the account belonging, the profiles of the users who are communicating, from which it is important to distinguish the Name, as well as the phone number of the users, if possible (identification of the party who is communicating and who enters into electronic transaction). Thus, when interviewing the applicant, the Notary should collect and reflect in the protocol the greatest amount of data, allowing the identification of the parties to electronic communication. Nevertheless, the applicant should be alerted to some of the risks associated with the fact that, for example, simply providing a person's last name, first name, and middle name on the record may not be an adequate identifier of the counterparty. Without passport information in the account, such correspondence may be questioned by a court as to its credibility and, therefore, there is a risk for it of being found defective on the grounds of the rules of relevance of evidence. Linking to a cell phone also does not seem to be a reliable identifier, since correspondence may be carried out by a person who does not own a SIM card. There is still a situation where a parent buys his/her underage child a SIM card for the phone in his/her name, and the child continues to use it even after the age of 18. Such a confluence of circumstances forces a critical attitude to cell phone numbers as a sufficient means of identifying a person in civil and other legal relations.

During the examination of the messenger, as a rule, the Notary examines the cellular phone and records its model, identification number and the number of the subscriber (applicant) himself/herswlf. However, the certification of legally significant information in the messenger is preferably performed on the notary's computer, which reduces the risks of prepared substitution of the certified information on the phone, and the distortion of the correspondence time by the device clock.

It is important to clarify with the applicant whether significant documents were exchanged in the course of the correspondence. If there are such documents, they must be uploaded by a notary, described, certified and also attached to the protocol. If there is an array of data, files, significant volumes of texts, they may be written down on digital media not subject to editing (e.g., CD disks), described in the protocol, and sealed in envelopes by Notary Public.

In any case, it is critical to record in the protocol of the examination the details: from which device the user was authorized (computer, cell phone), through which number correspondence took place (there are phones with two SIM-cards, or if it is a fixed network - SIM-cards with two subscriber numbers),

who owns the number through which communication took place, information about the profile of the parties, the name of messenger, etc.

The Notary Public shall inspect the mailbox and correspondence therein upon the request of the petitioner, provided that the request contains the information about the ownership of the mailbox by the petitioner, login and password providing access to the mailbox account.

When examining postal correspondence, the identification of the parties to the correspondence, the date, time, and content of the correspondence must be reflected in the notary's inspection report. The applicant must be warned of the need to record the correspondence in amounts that allow the court to reliably interpret the will of the parties. Partial certification of correspondence can be not only a method of falsification of evidence, but also a typical mistake made in securing electronic evidence and its subsequent rejection by the court on the objection of the defendant at the stage of their evaluation.

When notarizing legally significant electronic messages and actions testifying to a transaction, issues of compliance with its written form, generating obligations of the parties, it is necessary to take into account that electronic traces must contain the essential terms of the contract and expressed in the forms prescribed by law.

Thus, the existence of the transaction itself, as well as compliance with the requirements for its written form, can be proved through notarization of an electronic document exchanged by the parties (on the basis of article 434 of the Civil Code of the Russian Federation, the simple written form of the contract is considered to be observed if the contract was concluded as an electronic document signed by the parties, or the exchange of letters, telegrams, electronic documents or other data. At the same time, according to Article 160 of the Civil Code of the Russian Federation, any method that allows to reliably identify the person who expressed the will, not just a qualified enhanced signature (unless otherwise provided by law or contract) is equal to a signature (party identification (Blanchette, 2012; Voznesenskaya, 2022).

Also, proof of existence and execution of the transaction, and compliance with its written form is the notarization of electronic traces, i.e. actions to fulfil the conditions of the contract specified in the offer (a message on shipment of goods, services, works, transactions for the payment of the amount of the transaction, etc.) which are considered acceptance, unless otherwise provided by law, other legal acts or not specified in the offer (Nakhova, 2022).

Separately we should emphasize the importance of determining the parties in the exchange of legally significant messages that give rise to contractual consequences. According to article 165.1 of the Civil Code of the Russian Federation, statements, notifications, notices, demands or other legally significant messages, with which the law or the transaction binds civil-law consequences are recognized as such messages. As noted in this regard in paragraph 65 of the Resolution accepted by the Plenum of the Supreme Court of the Russian Federation dated 23.06.2015 N 25 "On application by the courts of certain provisions of Section I, Part I of the Civil Code of the Russian Federation", a legally significant message may be sent, including by e-mail, fax or other communication, and may be carried out in another form appropriate to the nature of the message and relations, information about which is contained in such communication, when it can be reliably established from whom the message came and whom it is addressed to.

CONCLUSION

Civil legislation based on the principle of dispositive behaviour of parties in private-law relations and the autonomy of will of participants of civil legal relations, acting in a rapidly changing world, taking into account the diversity of mechanisms used by participants of market relations, seeks to maximally normatively correspond to such existing and newly emerging legal relations and applied novelties of business turnover, evidence of which, for example, is introduced in the text of the Civil Code of the Russian Federation, article 141. The foregoing predetermines the need for readiness of the judicial system, procedural laws and notaries to record and take into account such innovations, since the implementation of such rights by participants of business relations (and not only) entails the occurrence of civil law consequences, the results of which may become the subject of a dispute in court. Accordingly, the Russian regulatory system must have mechanisms for fixing traces of such civil activity in order to use them as evidence in civil and arbitration disputes.

Obviously, while seeking to ensure the reliability of electronic evidence, notarial practice is now going in three directions of making protocols for recording electronic evidence:

1. Notaries with digital competence shall independently inspect sources of digital information using special software;
2. The staff of Notaries Public employees shall include an appropriate specialist as part of the employment relationships;
3. The Notary initiates a specialized (computer-technical) expertise to perform analysis of the most technically complex digital traces.

In fact, today we can talk about the formation of the need for the development of hybrid legal education, demanded, among other things, in the notarial practice of providing electronic evidence. The rapid development of electronic document flow, online conclusion of transactions, borrowing of foreign digital business and legal mechanisms only further testify to the need for further research of the mentioned topic.

ACKNOWLEDGEMENT

This article was prepared with the financial support of the RFBR grant No. 19-011-00820 (a) “The legal policy of the Russian State, its priorities and principles in the digital economy and the digital technological structure: conceptual, methodological, sectoral aspects of digitalization of law and legal regulation”

REFERENCES

Blanchette, J. F. (2012). Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents. MIT Press.

Golubeva, N., & Drogoziuk, K. (2019). Web-page screenshots as an evidence in civil procedure of Ukraine. Masaryk UJL & Tech., 13, 87.

Goncharova, M. V., Smirenskaya, E., Strokina, M., & Didenko, O. (2019). Electronic notary: The development of juridical on-line services in modern Russia. In Ubiquitous Computing and the Internet

of Things: Prerequisites for the Development of ICT (pp. 229-237). Springer, Cham.
Kashanin, A., & Churakov, V. (2021). Issue on “Small” and Indisputable Cases in Russian Courts. Global Jurist, 21(1), 273-303.
Nakhova, E. A. (2022). The comparative analysis of the law of evidence in civil proceedings in France and Russia. Вестник Санкт-Петербургского университета. Право, 13(1), 257-270.
Polina-Stashevskaya, A. L. (2022). Some Issues of Proof in Insurance Disputes in the Conditions of Digital Transformation of Law in Russia. In New Technology for Inclusive and Sustainable Growth (pp. 85-91). Springer, Singapore.
Rusakova, E. P., Frolova, E. E., & Gorbacheva, A. I. (2020, March). Digital rights as a new object of civil rights: issues of substantive and procedural law. In 13th International Scientific and Practical Conference-Artificial Intelligence Anthropogenic nature Vs. Social Origin (pp. 665-673). Springer, Cham.
Rusakova, E. P., & Frolova, E. E. (2019, October). Procedural aspects of proof in China’s internet courts: opportunities for receiving BRICS jurisdiction. In Institute of Scientific Communications Conference (pp. 1598-1605). Springer, Cham.
Smirenskaya, E., Kalashnikova, N., Osadchenko, E. O., & Tokarev, D. A. (2019). Electronic notary in modern Russia: A new juridical significant form of documents. In Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT (pp. 195-203). Springer, Cham.
Tarakanov, V. V., Inshakova, A. O., & Dolinskaya, V. V. (2019). Information society, digital economy and law. In Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT (pp. 3-15). Springer, Cham.
Tokarev, D. A., Usanova, V. A., Kagalnitskova, N., & Sandalova, V. A. (2019). Development of E-justice in Russia: Modernization of legal regulation and deepening of scientific research. In Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT (pp. 215-222). Springer, Cham.
Voznesenskaya, L. N. (2022). Impact of UP-TO-DATE Technologies on Efficiency of Corporate Disputes Examination in the Russian Federation. In New Technology for Inclusive and Sustainable Growth (pp. 249-259). Springer, Singapore.
Yakupov, A. G., Kirillova, E. A., Okriashvili, T. G., & Pavlyuk, A. V. (2020). Legal status, role and features of electronic document management. Utopia y Praxis Latinoamericana, 25(12), 178-186.