ЭКОНОМИКА И ПРАВО

УДК: 346.1

Solovyanenko N. I. The use of electronic documents and electronic signatures in digital economy: issues of legislation and legal practice

Solovyanenko Nina Ivanovna,
PhD, Legal Sciences, Senior Research Fellow,
Business and Corporate Law Department,
Institute of State and Law RAS

Abstract. *The article is devoted to the use in the digital economy of such legal instruments as electronic documents and electronic signatures, which protect the interests of market participants, the security of their information and ensure confidentiality. Among the main legal problems that need to be solved is to ensure the legal validity of documents and, accordingly, the credibility of them in the digital environment. Lack of trust is a fundamental barrier to the development of the digital economy. A strong legislative framework is needed to expand digital commercial operations. Therefore, the legal categories of electronic document and electronic signature are constantly being improved. The legal environment of trust in electronic documents and electronic signatures is formed both at the level of the internal legislation of the Russian Federation and at the level of regulatory acts of the Eurasian Union.*

Keywords: *entrepreneurship, digital transformation, electronic document, electronic signature, legal regulation of the use of electronic signatures, electronic business transactions, trust services, digital security and privacy, legal environment of trust.*

Рецензент: Рехтина Ирина Владимировна – кандидат юридических наук, доцент.
ФГБОУ ВО «Алтайский государственный университет»

Introduction

In the modern economy, the legal regulation of business activities is undergoing a digital transformation. The creation of legal rules governing the electronic interaction of business participants is a necessary condition for the development of entrepreneurship in the digital environment [4]. At the same time, uncertainty about legal regulation is one of the significant obstacles to the implementation of digital commercial operations both at the state level and at the international level. The main legal challenge that needs to be addressed is to ensure the credibility of legal interaction in the digital economy [5]. Lack of trust is a cardinal barrier to digital entrepreneurship. The participating States of the Organization for Economic Cooperation and Development (OECD), addressing the key challenges of the digital economy in 2016-2017, emphasized the need to «ensure trust; manage the risks of digital security and privacy» [8].

To perform legal interaction in the digital environment, special legal constructions are used, such as electronic documents and electronic signatures, which ensure the protection of

the interests of market participants, the security of their information and the preservation of confidentiality. The legal meaning of ensuring trust in electronic documents and electronic signatures used in business activities is to confirm their authenticity [2], reliability, immutability in the process of transmission from one participant of electronic interaction to another, as well as to maintain the legal force of such a document in the process of circulation or in the conditions of operational and/or archival storage.

Results and discussion

The functioning and development of digital markets requires a strong legislative framework [5]. Modern regulation should be based on the recognition of the freedom to choose the appropriate technologies, identification [3] and trust services, as well as the entities that provide them. At the same time, the provisions on the compliance of the applied technical and organizational means with national and international legal norms and standards must be observed. However, regulation may also include restrictions and burdensome conditions that make it difficult to conduct digital commercial transactions and, consequently, complicate the turnover of goods and services.

The legal principles developed by the United Nations Commission on International Trade Law (UNCITRAL) are the conceptual framework for regulating the use of electronic documents and electronic signatures [9]. Such principles are non-discrimination, functional equivalence and technological neutrality, which are widely regarded as the founding elements of modern electronic commerce law. The principle of non-discrimination ensures that a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality mandates the adoption of provisions that are neutral with respect to technology used. In light of the rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. The functional equivalence principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfil the same purposes and functions that certain notions in the traditional paper-based system - for example, writing, original, signature and record.

These principles are enshrined in the Model Law on Electronic Commerce, the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005) The UNCITRAL Model Law on Electronic Signatures (2001); the UNCITRAL Model Law on Electronic Transferable Records (2017).

In the Russian Federation, these principles are enshrined in the Federal Law "On Electronic Signature". These include : 1) the right of participants in electronic transactions to use an electronic signature of any kind at their own discretion, if the requirement for the use of a specific type of electronic signature is not provided for by law or agreement; 2) the

possibility of using any information technology or technical means to meet the requirements of the law " On Electronic Signature»; 3) electronic signature shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the electronic form .

Electronic signatures are essential for digital business. The legal significance of digital documents that are used in the course of electronic business transactions, as a general rule, depends on the results of the use of electronic methods of authenticating such documents. The concepts of «document» and «signature» are interrelated and legally complement each other [1]. A number of laws emphasize the informational nature of an electronic document and an electronic signature. Within the meaning of Federal Law of July 27, 2006 N 149-FZ «On Information, Information Technologies and Information Protection» an electronic document is information in electronic form, that is, in a form suitable for human perception using electronic computers, as well as for transmission over information and telecommunications networks or processing in information systems. However, the Civil Code of the Russian Federation emphasizes the legal role of an electronic document and an electronic signature. In accordance with Part 2 of Article 434, an agreement in written form may be made by drawing up a single document (including an electronic one) signed by the parties thereto or by exchanging letters, telegrams, electronic documents or other data.

An electronic signature usually performs the following legal functions, but is not limited to:

- indicates who signed the electronic document,
- ensures that the electronic document is signed by a duly authorized person;
- ensures the authenticity and immutability of the signed document;
- represents the signer's expression of will;
- represents the required written form of the document.

Signing a contract as a way of accepting its terms brings the necessary certainty to the transaction [6]. Otherwise, the parties may ignore the terms of the transaction, not considering them as legally binding. Signing digital documents with an electronic signature provides such electronic documents with guarantees against unauthorized access by third parties or against forgery.

In the UNCITRAL materials related to the development of the Model Law «On Electronic Signatures», digital signatures are considered as functional equivalents to handwritten signatures. «Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form. Digital signatures use what is known as «public key cryptography», which is often based on the use of algorithmic functions to generate two different but mathematically-related «keys» (Le., large numbers produced using a series of mathematical formulae applied to prime numbers). One such key is used for

creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as cryptosystems or, more specifically, asymmetric cryptosystems where they rely on the use of asymmetric algorithms ».

The Federal Law provides for a simple electronic signature and an advanced electronic signature, as well as qualified electronic signature.

A simple electronic signature is an electronic signature that, through the use of codes, passwords, or other means, confirms the formation of an electronic signature by a certain person.

Advanced electronic signature: 1) obtained as a result of cryptographic transformation of information using the electronic signature key; 2) allows you to identify the person who signed the electronic document; 3) allows you to detect the fact of making changes to the electronic document after signing it.

A qualified electronic signature corresponds to all the features of an advanced electronic signature and the following additional features: 1) the electronic signature verification key is specified in a qualified certificate; 2) for the creation and verification of an electronic signature, electronic signature means are used that have proof of compliance with the requirements established in accordance with this law.

Information in electronic form signed with a simple electronic signature or an advanced electronic signature is recognized as an electronic document equivalent to a paper document signed with a handwritten signature, in cases established by federal laws, other regulatory acts, regulatory acts of the Central Bank of the Russian Federation or an agreement between participants in electronic interaction, including the rules of payment systems. For example, the Law of the Russian Federation " On the Organization of Insurance Business in the Russian Federation provides that in the implementation of compulsory insurance, the recognition of information in electronic form signed with a simple electronic signature, an electronic document equivalent to a paper document signed with a handwritten signature, is established by federal laws on specific types of compulsory insurance and regulatory acts of the insurance supervisory authority adopted in accordance with them. When implementing voluntary insurance, such requirements and procedures are established by the insurance rules or other agreement between the specified persons.

In accordance with the legislation of the Russian Federation, a qualified electronic signature is characterized as the most reliable, legally guaranteed type of electronic signature. An electronic document signed with a qualified signature has the same legal force as a paper document signed with your own hand. For example, to perform notarial actions with

documents and transfer information to the unified information system of the notary, the notary uses a qualified electronic signature.

The Federal law gives legal meaning to the technological and organizational procedure for forming an electronic signature (signing an electronic document) and verifying it with the help of an electronic signature verification key certificate. The certificate of the electronic signature verification key is created and issued by the certification authority. Thus, a qualified electronic signature is recognized as valid if the following provisions are simultaneously observed: 1) the qualified certificate is issued by an accredited certification center; 2) the qualified certificate is valid at the time of signing the electronic document or on the day of verification of the specified certificate, if the time of signing the electronic document is not known; 3) as a result of verification, it is confirmed that the qualified electronic signature with which the electronic document is signed belongs to the owner of the qualified certificate, and also confirmed that there are no changes made to this document after its signing.

The legal categories «electronic document» and «electronic signature» are constantly being improved by the legislator.

The issues of forming the legal regime of electronic (digital) documents and its constant updating occupy a sufficient place among the tasks of the federal project "Legal Regulation of the Digital Environment". The draft provides for clarification of the concept of an electronic document; definition of the terms «electronic duplicate» and «electronic image» of a document; as well as regulatory consolidation of procedures for the use and storage of electronic documents, the production of notarial documents in electronic form; registration of the legal status of electronic systems for recording legal facts. In addition, in the field of digital interaction between the business community and the state, the project involves maintaining electronic personnel document management, including accounting for information about the employee's work activity through an electronic record; conclusion, amendment, termination of employment contracts in electronic form. The latest legislative changes in this area indicate not only the expansion of the concept of «electronic document» and the expansion of the corresponding legal structure, but also demonstrate the active promotion of electronic document management by the legislator as the main method of performing legal interaction in the economic and social sphere. This trend has significantly increased due to the objective need to carry out «contactless» business interaction in the context of the pandemic. As for document management «on paper», which do not meet the innovative needs of digital communication and are difficult to implement during the «lockdown» period, they are considered in modern rulemaking, rather, as an exception. There are new types of relations and concepts that did not exist during the active formation of the current regulatory framework: visualization of an electronic document and an electronic signature, conversion and migration

of electronic documents, digital three-dimensional models of intellectual property objects, cloud-based (remote) qualified electronic signature.

It is necessary to emphasize the addition to the Law on Electronic Signature, which provides for a new legal structure, the so-called trusted third party. The legal function of a trusted third party is to verify electronic signatures in electronic documents at a fixed time, as well as to confirm the results of such verification. A trusted third party performs the following legal functions:

- confirms the validity of electronic signatures and certificates for electronic documents at a certain time, as well as the issuance of the latter by accredited certification centers;
- checks the compliance of all qualified certificates used when signing an electronic document with the requirements of the legislation;
- verifies the credentials of the participants in the electronic interaction; creates and signs a receipt with the result of the verification with a qualified electronic signature of a trusted third party;
- stores data about operations performed by a trusted third party.

These activities can be carried out by legal entities after obtaining the appropriate accreditation.

The legal construction of the trusted third party is designed to strengthen trust between participants in electronic interaction and provide new tools for resolving conflict situations related to the use of electronic signatures and confirmation of the powers of participants in electronic interaction [7]. The trust is based on state accreditation and control over the activities of a trusted third party.

A trusted third party is a central element of the legal model of the digital environment of trust, which is formed at the domestic level, as well as at the cross-border level, primarily in the integration associations of States.

The Treaty on the Eurasian Union provides the basis for the legal regulation of electronic document management with the participation of the Eurasian Economic Commission, state authorities of the member States of the Union, private legal entities and individuals. The Treaty on the Eurasian Union also provides for the creation of an information structure for the interstate exchange of data and electronic documents for the purpose of integration cooperation within the Union. The member States of the Union and the Eurasian Economic Commission are forming a cross-border environment of trust in electronic documents and electronic signatures, the legal basis of which is the strategy and concept of using legally valid electronic documents and services in interstate interaction. The conceptual approach to the use of electronic documents in the EAEU includes the following fundamental legal positions developed in international model laws: a) an electronic document drawn up according to the rules approved by the Eurasian Economic Commission is recognized as equal in legal force to

a similar document on paper, certified by a handwritten signature or signature and seal; b) a document cannot be deprived of legal force on the sole basis that it is drawn up, sent or received, as well as stored and used in electronic (digital) form.

The decision of the Board of the Eurasian Economic Commission No. 125 of September 28, 2015 approved the Regulation on the exchange of electronic Documents in the cross-border interaction of public authorities of the member States of the Eurasian Economic Union among themselves and with the Eurasian Economic Commission. The regulation establishes the rules for the exchange of electronic documents within the framework of the integrated information system of foreign and mutual trade; determines the composition of participants in the exchange of electronic documents; general requirements for electronic documents; requirements for signing an electronic document with an electronic digital signature, as well as establishes the responsibility of participants in the electronic document flow. The Regulation provides for such a technological and legal structure as the «service of the trusted third party of the integrated system», which is a set of services of the trusted third party of the member States and the Eurasian Economic Commission that provide a cross-border environment for the exchange of electronic documents.

Conclusion

Recent legislative changes, primarily forming the legal environment of trust, indicate the expansion of the concept of "electronic document" and the expansion of the relevant legal provisions and demonstrate the active promotion of electronic document management by the legislator as the main method of implementing legal interaction in the economic and social sphere. A modern regulatory approach to the legal regime of electronic documents should meet such requirements as functionality, dynamism and flexibility, updating the main legal models, creating fundamentally new concepts and legal provisions. At the same time, regulation should not create artificial barriers to innovation or increase the cost of implementing it.

References

1. Braginsky M. I., Vitryansky V. V. Contract law. General provisions. M., 1997. p. 226.
2. Minaev V. A., Korolev I. D., Sabanov A. G. Risk assessment of identification and authentication of subjects of electronic interaction// Bulletin of the Urfu. Security in the information sphere. 2018. No. 4 (30). pp. 43-49.
3. Naumov V. B. Problems of the development of legislation on the identification of subjects of information relations in the digital economy //Proceedings of the Institute of State and Law of the Russian Academy of Sciences. No. 4/2018. pp. 125-151.

4. Plotnikov, V. A. Digitalization of production: theoretical essence and prospects of development in the Russian economy / V. A. Plotnikov // Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta. – 2018. – № 4 (112). – Pp. 16-24.
5. Shapsugova M. D. Implementation of the principles of digital economy and smart contract technology in the legal regulation of business activity// North-Caucasian Legal Bulletin. 2018. No. 2. pp. 76-82.
6. Digital Regulation Handbook: Geneva: International Telecommunication Union and the World Bank, 2020. Licence: CC BY-NC-SA 3.0 IGO.
7. Draft Provisions on the Cross-border Recognition of IdM and Trust Services. URL:<https://undocs.org/en/A/CN.9/WG.IV/WP.157>.
8. OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris. 21-38 DOI: <https://dx.doi.org/10.1787/9789264276284-en>.
9. Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf