

# *The impact of the digital economy on the development of Russian law*

Vladimirov I.A.  
Bashkir State University  
Ufa, Russia,  
[docentufa@mail.ru](mailto:docentufa@mail.ru)

Iksanov R.A.  
Bashkir State Agrarian University  
Ufa, Russia,  
[iksanov333@yandex.ru](mailto:iksanov333@yandex.ru)

Rashitova L.K.

Bashkir cooperative institute (branch) of the autonomous non-profit educational organization of higher education of the Central Union of the Russian Federation "Russian University of Cooperation"  
Ufa, Russia,  
[irashitova@rucoop.ru](mailto:irashitova@rucoop.ru)

**Abstract** — The article reveals the impact of the digital economy on the development of certain branches of Russian law, regulating a particular particular sphere of public relations. digital identification to improve existing mechanisms to protect the rights of digital users.

**Keywords** — digital economy, law, digital identity, digital money, online fraud, electronic digital signature.

## I. INTRODUCTION

In the digital economy, law remains one of the main regulators of public relations. The digital economy creates the basic conditions for the development of society and all sectors of the economy through digitalization and digital transformation processes. The digital economy is not a separate sector of the economy, as it affects all areas of society, including social sphere and public administration.

At the moment, Russia needs to adopt new legislation regulating digital relations, detail ingeshers and specificity of the already adopted regulatory framework. The lack of effective legislation is actively used by Internet fraudsters, in affecting ingesising the property, intellectual and other rights of citizens and organizations. Along with the development of digital technologies, new types of delinquency are emerging. The legal responsibility of the actors in the digital economy has not been resolved. This necessitates adapting Russian law and the entire law enforcement system to new, changing conditions of the digital economy.

## II. RESULTS OF THE STUDY

### A. Method of analysis of legal norms.

Analysis of the provisions of the current legislation reveals the meaning of the legal norm to determine the extent of its impact on the development of relations in the digital economy.

### B. The method of law enforcement analysis.

The works of foreign authors on the subject under study have been studied.

## III. THE RESULTS OF THE STUDY

To carry out these processes, Russia has launched a national program called The Digital Economy of the Russian Federation, which is managed and administered by the Ministry of Digital Development, Communications and Mass communications of the Russian Federation. This project creates the conditions for the development of the digital economy. One of the conditions for the effective development of the digital economy in Russia is the presence of developed infrastructure, i.e. systems of fiber optic networks, cellular and other types of communication, which provide access to the Internet. The digital economy is influenced by human resources. Without the availability of competent personnel, it is not possible to develop the digital economy in various fields.

To the obligatory condition of the development of the digital economy is information security - a state of protection of vital interests of the individual, society and the state from external and internal information threats. Information security provides users with internet security, safe use of software. The Russian Federation's Information Security Doctrine, approved by Decree of the President of the Russian Federation No.646 of December 5, 2016, stipulates the need to link information security before the introduction of information technology. One of the areas of information security in the globalized information world should be the introduction of domestic digital technologies through the import substitution programme.

The direction of the national project "Digital Public Administration" implemented on a regional scale in Russia is carried out in the context of transformation of the state administration itself and interaction with citizens.

The national project "Digital Economy of the Russian Federation" may appear two new directions: "Smart City" and "Digital Medicine." The President has repeatedly mentioned the need to translate our daily lives into a number in the Address to the Federal Assembly. In the Message, the President of the Russian Federation set the task of bringing developed communications to small towns and villages of the Russian Federation, eliminating digital disparities between the city and the village in Russia. The simplest example where much has already been done in the digital sector is mobile communication. By 2024, the country should have almost universally fast Internet access.

The digital economy is a powerful driver for the development of the country's economy as a whole and all industries, from agriculture to space activities. The key question is how to apply in practice the digital economy that has already been successfully implemented in other parts of the world and is being used everywhere by both government and business.

The opportunities and advantages of the digital world include the development of telemedicine, online education, remote provision of public and municipal services in real time, ordering almost any type of goods. The shortcomings of the digital economy include the unpreparedness of the human rights and law enforcement system of the state, the vulnerability of vulnerable categories of the population to new challenges in the digital economy.

First of all, it is necessary to define the regulatory and regulatory sphere of the digital economy, because so far 90% of the entire digital economy and all new technologies that need to be used are outside the legal field. In the Russian Federation, all market participants in the digital economy are waiting for legal regulation to be determined in order to eliminate risks in their activities and to take full advantage of the opportunities provided.

We believe that in order to define regulation it is necessary to study and take into account positive foreign experience. China and the United States are currently considered to be the leading countries in the digital economy. The Russian Federation has every opportunity to take its rightful place among the world leaders in e-commerce and cross-border trade. The development of jurisprudence in the digital economy has been studied in the works of foreign researchers: Claire Sullivan, Graham Horsman, Uta Coel, etc.

The regulatory framework governing the digital economy is the Russian Civil Code, which, from October 1, 2019, enshrines a new object of rights - digital rights, which are understood to be obligations and other rights, content and conditions implementation of which is determined in accordance with the rules of the information system, which meets the statutory criteria. The digital economy is already concerned with any interaction between man and the state. The regulatory framework for the digital economy also includes the Federal Act of 06.04.2011 No. 63-FH "On Electronic Signature", which, in our opinion, needs to be amended to prevent abuse of electronic digital Signature. In the absence of effective digital legislation, citizens risk losing not only all their savings, but also real estate. In practice, there

are cases when citizens suddenly find themselves big businessmen who own dozens of bankrupt firms. Criminals have learned to forge electronic signatures and victims of scams learn too late that they have suffered from cyber-fraudsters.

Fraudsters safely use passport data and other personal data that are freely available in the Internet space. E-signature fraud in 2018 has become three times more popular than in 2017.

To obtain an electronic digital signature at the moment you need to provide ANIN, SNILS and a real passport. If the fraudster managed to find the real series and number and made a paper document, he gets the opportunity to make financial transactions on behalf of another person. Unsuspecting people are issued one-day companies, which are designed for a one-time withdrawal of funds to offshore. As a rule, a firm is created to evade taxes, to deal with cashing, legalization of criminal proceeds. In the near future, the increase in offences in the field of certifying centers is projected. It is becoming increasingly difficult for the law enforcement system to control this area. We believe that it is necessary to reduce the number of certifying centers, to tighten the responsibility of the employees of these centers for improper performance of their duties, for the disclosure and transfer of personal data of citizens. To identify the scammers, it is necessary to provide access to the staff of the certifying centers, issuing electronic digital signatures to more accurate information databases with photos of Russian citizens, for their further digital identification.

#### IV. THE DISCUSSION OF THE RESULTS.

Digital identification is an identity that consists of information stored and transmitted digitally. Countries around the world are translating services and transactions into online mode, and digital identification is being introduced into the fundamental processes needed to ensure economic and social order.

Overseas, an individual must use this government-appointed digital identification to access these services and conduct transactions under the e-government scheme. As international experience has shown, the e-government scheme is likely to set the standard so that the same digital ID will be used for transactions in the private sector.

This means that, in fact, this digital identity becomes the primary means by which an individual makes transactions in the digital age. As digital identity becomes more and more important, both commercially and legally, the law is looking for ways to adequately protect this new concept and the human interest in it. Legislators are now trying to find an effective way to recognize mutual rights and responsibilities regarding digital identity. Given the legal and commercial importance of digital identity and the impact of its compromising on humans, current civil, criminal, administrative and other forms of legislation do not adequately recognize and protect rights and interests of man.

The digital identification required for transactions has a specific legal provision. Using digital identification to make transactions makes it both valuable and vulnerable.

Identity information that links registered digital identification to a person is particularly prone to errors and fraud. However, the system is designed so that all transactions that use digital identification are automatically attributed to the person to whom it is registered under the scheme, regardless of whether or not the person has actually used the scheme identification to make a deal. This can have significant consequences for all users and have implications for the integrity of the scheme, but the consequences are most immediate and serious for the innocent person. Today, legal science and jurisprudence rely on confidentiality to protect personal information. Privacy, by its very nature, cannot adequately protect the part of digital identity required for transactions because of its inherently public nature. C.

Sullivan argues that the right to identity can and should be recognized to fully protect human rights under this scheme, especially in view of the inherent errors in the scheme.

Individual rights in the digital economy can easily be used to recognize and protect a person's rights and interests in a digital citizen's identity card under a government electronic IDENTITY scheme. The protection of individual rights is important given the nature and functions of this digital identity and the harm caused to man by its compromising. Legal protection of subjective civil rights with the participation of business entities in the field of monetary relations is carried out by various legal means, the central place of which is the legal means of civil law, writes Safin F.F. Conceptually, individual civil rights provide a more reliable basis for protection than the current reliance on privacy and criminal law. The nature of these rights and their historical international influence make them a workable model for both the civil and other legal systems.

Australia is the first country to formally recognize the importance of digital identity and raise the issue of reciprocal rights and responsibilities between the State and its citizens. It is this country that can be considered the birthplace of digital citizenship. Given the increasing commercial and legal importance of the implications for individuals, the right to identity as an international fundamental human right must now be recognized and protected against digital identity.

Recognition and protection of this right are an important component of the model of responsible digital citizenship. Recognition of the right is one of the ways to protect the civil rights provided by Art. 12. Ustyukova V.V. points out that the recognition of the right removes doubts about the ownership of the right to a person.

Despite the perfection of new technologies from the actions of Internet fraudsters suffer tens of thousands of Russians recklessly make deals and massively lose money, which with rare exceptions is impossible. Russian legislation loosely regulates the Internet environment. Russia's legislature is puzzled by its regulation. The content of the Russian Civil Code, the second most important document, after the Russian Constitution, regulating the digital economy, is constantly

changing. In the Russian Central Committee, there will be a new chapter that enshrines the concept of digital rights. The consolidation of the basic concepts of a fundamentally new field of wires will give a boost to the development and improvement of digital legislation. The Digital Rights Bill is laying the groundwork for the development of the digital economy. Digital rights are a new area for Russian law, so it is important to enshrine basic concepts. The Internet environment will begin to obey not only unwritten laws, but also quite clear specific legal norms, the average user and enterprising businessmen will get confidence in their actions and guarantees of protection of rights in case of unforeseen circumstances. Relationships in the Internet environment will cease to be no control, unknown gray zone. The user's personal information becomes, in fact, the key to material values.

The issue of personal data protection is governed by a special law. In most cases, personal data on the Internet is needed for so-called smart contracts, i.e. direct transactions without the participation of intermediaries. elements of legal regulation in this area. Their implementation is a computer algorithm: become everyday car payments for utilities or bank transfers - any transactions the state will recognize. transactions, such as sales, leases, contracts, deliveries, and so on. The law will apply to financial transactions, the activities of large commercial organizations and even the will of the voters and other equally vital things, such as absentee participation of the shareholder in meetings, in voting (referendums and elections) and so on

Initially, the legislative initiative touched on another important object - virtual monetary relations, cryptoindustry. The concept of digital money and how to use it were introduced. However, by the second reading of the bill, the cryptocurrency clause was removed. If the legislation of more than a dozen countries managed to painlessly prescribe the rules of regulation of the market of virtual money, in Russia for this purpose to make changes in the main state document - the Constitution of the Russian Federation. Article 75 of the Russian Constitution stipulates that the currency in the Russian Federation is the Russian ruble. The issue of funds is carried out exclusively by the Central Bank of the Russian Federation. From this we can conclude that the introduction of other money emissions in the Russian Federation is not allowed.

Offences in the digital economy and high information technology are investigated and disclosed by specialized operational units whose officers identify and cross illegal activities related to creation, disruption, processing and improper access to legally protected computer information, the creation, distribution and use of malicious computer programs, violation of the rules of operation of the storage facilities for processing or transmitting computer information. In the digital economy, the fight against Internet fraud, theft of money from plastic cards and illegal trafficking of special technical means intended for the secret receipt of information, crimes related to crimes related to the illegal use of cellular and wired network resources, and improper access to commercial satellite and cable television channels.

Offenders have learned not only to forge an electronic digital signature, but also to deprive citizens of real estate, including the only housing. In the Russian Federation, cases of weaning of apartments by falsification of electronic digital signatures are recorded. So a resident of Moscow discovered that the next receipt for utilities at the apartment indicated a new owner. The citizen turned to the Rosreester and found out that he had given his apartment to a Ufa resident in the autumn of 2018, and he did it remotely by signing documents with an electronic digital signature. At the same time, the victim himself stated that he had never issued an electronic signature at all and had never received a physical carrier of EDS. However, this did not prevent the scammers to officially register the deal. The victim appealed to the IFC and received an extract from the EGRN, which stated that on October 22, 2018, he gave the apartment to a resident of Ufa. The Rosreestre officially confirmed that the property was indeed donated. The documents were submitted electronically by a digital signature and everything is perfectly legal. The scammers received electronic signatures through their personal office on the portal of the State Service. The transfer of the property was carried out not as a sale, but as a gift without the participation of a notary. The gift agreement is signed on both sides by electronic signatures. A fraud report has been filed with the police, investigations and search operations are underway.

Offenders have learned to make real estate transactions by gaining access to an electronic signature and having issued it with only 2 documents: copies of the passport and SNILS. At the same time, property owners may have papers on ownership, but it is almost impossible to prove that the owner did not sell, transfer, give his property. Scammers also use old passport data, expired documents, and the owner may not have an electronic signature in the database and learn about the scam only after receiving a receipt for someone else's name.

Unfortunately, even having a statement about transactions only in a personal presence does not guarantee full security. A system designed to make people's lives vulnerable. In practice, the risk of obtaining an electronic signature verification key by an outsider is quite high, experts say. In addition to real estate transactions, digital signature can be used for remote processing and other documents, including lending, registration of a legal entity and so on. Citizens with real estate have the opportunity to impose a total ban on real estate transactions by making it through a simple procedure: contacting the IFC with a passport and in the presence of a center employee having written an application for a ban on the ban on conduct any any registration actions with real estate without a personal presence in a free form with the presentation of legal documents.

The law on electronic signature it should protect Russians from real estate fraud now when buying an apartment sale using new technologies will need to notify the Rosreester to file an application can in any center of state services termination of the right

In Russia, from August 13, 2019 came into force the law on real estate transactions with electronic signature now it is impossible to remotely apply for registration of real estate

transactions without the written consent of the owner. These innovations should protect citizens from fraud. In the application procedure, it will be possible to make a record of the possibility of registering the transfer of ownership of the property only on the basis of an electronically certified electronic application. In the absence of such a record in the EGRN to conduct a transaction remotely it is impossible. At the moment, accredited certifying centers are responsible for issuing electronic signature certificates for obtaining state services.

## V. CONCLUSIONS.

We believe that in order to determine the regulatory regulation of the digital economy, it is necessary to study and take into account positive foreign experience.

The authorities recognize that the problem is extremely dangerous. Changing the law is the exclusive competence of the Federal Assembly of the Russian Federation. The legislator was warned about possible gaps in the legislation, which will certainly be used by the legislator. The lower house of the Federal Assembly of the Russian Federation - the State Duma of the Russian Federation should begin to consider a number of bills that should block criminals' paths for real estate fraud using electronic digital signatures and tighten rules for certifying centers that are involved in the assignment of electronic digital signatures. It also appears that the number of certifying centres is reduced and the staff of these centres are held accountable for improper performance of their duties, for disclosing and transferring personal data Citizens.

In order to identify persons attempting to commit fraud, it is necessary to provide access to the staff of the certifying centers, issuing electronic digital signatures to more accurate information databases with photos of Russian citizens, for their further Digital identification.

## References

- [1] Passport of the national program "Digital Economy of the Russian Federation" (the Presidency of the Council under the President of the Russian Federation for Strategic Development and National Projects, protocol of 24.12.2018 No. 16) / SPS Consultant.
- [2] Decree of the President of the Russian Federation dated 05.12.2016 No. 646 "On the Approval of the Doctrine of Information Security of the Russian Federation" / SPS Consultant.
- [3] Russian Presidential Address to the Federal Assembly dated February 20, 2019 / Russian newspaper, No 38, 21 February 2019.
- [4] Graeme Horsman. Can we continue to effectively police digital crime? // Science & Justice, Volume 57, Issue 6, 2017, Pages 448-454.
- [5] Uta Kohl. Chris Reed and Andrew Murray, Rethinking the Jurisprudence of Cyberspace (EE, 2018) // Computer Law & Security Review Volume 35, Issue 2, 2019, Pages 239-240.
- [6] The Civil Code of the Russian Federation (part one) from 30.11.1994 No. 51-Fz (ed. from 03.08.2018, with a.m. from 03.07.2019) / Russian Legislative Assembly, 05.12.1994, No. 32, art. 3301.
- [7] Federal law of 06.04.2011 No. 63-Fz "On electronic signature" (with iz. and dop., effective from 31.12.2017) / Parliamentary newspaper, No. 17, 08-14.04.2011.
- [8] Clare Sullivan, Sophie Stalla-Bourdillon. Digital identity and French personality rights – A way forward in recognising and protecting an

- individual's rights in his/her digital identity // *Computer Law & Security Review*, Volume 31, Issue 2, 2015, Pages 268-279.
- [9] Clare Sullivan. Digital identity, privacy and the right to identity in the United States of America // *Computer Law & Security Review*, Volume 29, Issue 4, 2013, Pages 348-358.
- [10] Safin S.F., Habibullina A.S. Role of civil-legal contracts in the production and sale of agricultural products / *Law and state: theory and practice*. 2014. No. 12 (120).
- [11] Clare Sullivan. Digital citizenship and the right to digital identity under international law // *Computer Law & Security Review*, Volume 32, Issue 3, 2016, Pages 474-481.
- [12] Ustyukova V.V. Recognition of law as a way to protect land rights / *Agricultural and land law*. 2016. No. 4 (136).
- [13] Safin S.F. To the question of the legal responsibility of economic entities of the agro-industrial complex in the field of monetary relations / *Herald of the St. Petersburg University of the Russian Interior Ministry*. 2005. No. 4 (28).