Digital Law and Digital Rights in Russia: Polemical Notes

Elvira Talapina

Chief Researcher, Doctor of Juridical Sciences, Doctor of Law (France), Institute of State and Law, Russian Academy of Sciences. Address: 10 Znamenka Str., Moscow 119019, Russian Federation. E-mail: talapina@hotmail.com

Abstract

Digitalization has become omnipresent today. No longer limited to the security sphere, digital technologies are actively transforming society as a whole. However, the conservative institution of law does not always respond promptly to changes, and many lawyers believe that the traditional legislation in force is sufficient to handle this new object of regulation. Yet the fact is that this object cannot be called traditional from the regulatory standpoint. Technology has a powerful impact on both law and the state and so requires new solutions. Under such circumstances, it is important to gain a legal understanding of digitalization without delay. The purpose of this article is to analyze the current state of legal regulation of digital technologies in Russia. By employing classical legal methods for analyzing doctrine, legislation and jurisprudence, the author comes to the conclusion that digital law is a new branch of law. At the same time, its most significant aspect is the regulation of digital rights — subjective rights associated with the use of digital technologies. Despite the neutral and universal character of technologies, a comparative legal approach allows us to identify the specific features of Russian digital law, as well as the nuances of the regulation and protection of digital rights in Russia. The present article reflects the author's position and strives to inspire further discussion about these issues.

Keywords

digital law, digital rights, digital data, technology law, neutrality, cyberspace.

For citation: Talapina E. (2021) Digital Law and Digital Rights in Russia: Polemical Notes. *Legal Issues in the Digital Age,* no 1, pp. 3–16.

DOI: 10.17323/2713-2749.2021.1.3.16

Introduction

While law does not always take a lot of interest in the development of digital technologies, it has, at least, begun to perceive them as an object of regulation today. The term "digital" is used on two basic levels in law:

the level of the legal regulation of digital technologies in general (blockchain, artificial intelligence, etc.) and the level of the protection of subjective rights. In this sense, it would be legitimate to talk about digital law as a regulatory area and about digital rights as subjective rights associated with the use of digital technologies in various areas of life. Let us examine how these two areas are developing in contemporary Russia.

1. Digital law

Today, digitalization is the most frequently mentioned global phenomenon that has a transformative impact on both the national and the global levels. Whereas digital information technologies were assigned a provisional, auxiliary status at their early stages of introduction, they have begun to play an independent role today, changing the structure of society in general and legal regulation in particular.

On the whole, lawyers react ambivalently to digitalization processes. There are two contrasting approaches that assess the ability of traditional law to meet technological challenges. The first, which may be called "technocratic," is based on so-called "cyberlibertarianism" [Tulikov A.V., 2016: 236]. According to cyberlibertarians, the role of traditional law is limited in the cyberspace due to the low regulatory power of national law. Since information is disseminated globally with no regard for national boundaries today, the role of the state is also diminishing. Cyberspace has its own rules that are determined by the technical processes of transferring and recording data. Thus, according to this theory, the value of law is significantly reduced in a digital environment. This approach has been greatly influenced by the theory of Lawrence Lessig [Lessig L., 1999], who pointed out that the regulation of activities in the cyberspace is carried out both through legislative acts (legal code) and through software/hardware (technical code). The second approach reflects the resistance of traditional lawyers to the digital offensive. In their opinion, law has faced a variety of challenges over the history of its existence — including technological challenges (for example, in private law, land ownership used to extend indefinitely upward into space; however, the emergence of civil aviation quickly changed the legal approach) — and sooner or later manages to "incorporate" emerging innovations into the mainstream of classical legal regulation. That is, law is a fairly dynamic system that is capable of developing and changing while maintaining its traditional features.

As is often the case, the approach that lies in the middle between two extremes may well provide the best description of reality. Let us formulate it

as follows: while the influence of digital technologies on law is indisputable, law has significant resources to treat digital technologies as an object of legal regulation. This is the most appropriate context for talking about digital law.

Before analyzing Russian digital law, we should mention the importance that Russian law in general attaches to the division of the legal system into branches. This tradition goes back to Soviet times and, more precisely, to the legal systematization carried out in the 1930s with the division of law into branches (civil, criminal, administrative, etc.) defined by fairly strict criteria. While this approach to the systematization of law is beneficial in many ways, its relevance, in our opinion, has been significantly reduced today. The sectoral division of law is overly ideologized [Yakovlev V.F., Talapina E.V., 2012: 6–8], and, rather than waiting for a particular branch or method to be formalized, it would be much more practical to proceed from the fact that a sphere of social life deserves special legal regulation for the simple reason that relations within it are already taking place with a certain frequency. There are no clear-cut boundaries between social relations or between the legal branches "dedicated" to them, and, thus, there are no uniquely applicable methods, either. While branches of law mostly follow legislation, there are no "pure" sectoral laws at all. Therefore, when demarcating types of relations for the purposes of their legal regulation, it is the subject rather than the method that matters; in any case, it suffices for assigning a certain degree of autonomy to a sphere of legal relations.

From this standpoint, the subject of digital law is relations involving the use of digital technologies. Such a description is, of course, extremely broad, because digital technologies are used in many branches of law — criminal, administrative, etc. (indeed, in every known legal branch). The excessively broad subject of digital law has evoked relentless criticism, as was the case with Internet law, which the American judge Frank H. Easterbrook jokingly called the "Law of the Horse." In his opinion, nothing prevents teaching "horse law" in law schools as a set of legal prescriptions (related to a wide variety of legal branches) applicable to all cases in which horses are the subject of relations (sale and purchase of horses, harm caused by horses, etc.), yet such a discipline would be blurred and devoid of unifying features [Easterbrook F., 1996]. Disagreeing with this view, Harvard professor Lawrence Lessig argued that this risk is absent in the case of cyber law, since the very architecture of the Internet has laid the foundations for such unifying features [Lessig L., 1999].

Thus, it is the basic technical features of digital technologies that allow one to talk about the demarcation of digital law today.

Discussions about digital law have intensified in Russian legal literature in recent years on account of the implementation of the Digital Economy national project. At the same time, the range of approaches to the definition of digital law in legal literature is quite broad, which suggests that this branch of law is still in its infancy (let us emphasize once again that we are not referring here to the traditional Soviet definition of a branch with an established subject and method). For example, in a textbook released by Kutafin Moscow State Law University, digital law is defined as a legal institution that represents a system of "generally binding, formally defined, state-guaranteed rules of conduct, which develops in the field of application of digital technologies and regulates relations arising in connection with the use of digital data and the use of digital technologies" [Blazheev V.V., Egorova M.A., 2020: 36].

Marina Rozhkova understands digital law as a set of legal norms and institutions regulating different relations associated with the introduction and use of digital technologies, emphasizing that these norms are not united by a single method of regulation and relate to various branches of law [Rozhkova M.A., 2020]. Some equate digital law with Internet law, calling its virtual character a characteristic feature of digital relations [Vasiliev A.A. et al., 2019: 17]. A narrower understanding of digital law corresponds to the cyberlibertarian position: digital law is a system of legal prescriptions set down by the state in a set of digital codes or designations through which social relations are regulated within the framework of information systems recognized by the state [Golovkin R.B., 2019: 166]. Finally, some authors simply reject the very existence of digital law: "as far as digital law is concerned, it must be considered to be a premature result of the search for a way to combine economics and law: indeed, it is nonsense, not reality" [Galuzo V.N., Kanafin N.A., 2018: 124].

In our opinion, such a diversity of views indicates that the new branch is currently emerging and looking for a place in the established legal system. At the same time, we believe that the existence of this subject of regulation — relations associated with the use of digital technologies — is difficult to call into question. The peculiarity of digital law is that the legal regulation of digital technologies exists in all branches of law. In particular, this circumstance explains the lack of a single method of regulation. As it was noted by Olimpiad Ioffe and Mikhail Shargorodsky, discussions about system of Soviet law analyzed the regulatory method only for administrative and civil law [Ioffe O.S., Shargorodsky M.D., 1961: 349]. Indeed, the development of legislation gradually led to the emergence of legal branches that were not characterized by the use of any one regulatory method (e.g.,

labor law and environmental law). Thus, long before digital law, the importance of the method of legal regulation in substantiating the independence of a branch of law was put into question.

Another feature of digital law is that it "oversteps" the boundaries between public and private law. Any cyber technology can be applied in both public and private legal relations. The emerging regulation of technology *per se* often liberates public and private law from developing their own approaches. Or such regulation develops where it originally originated (most often in private law). For example, smart contracts that have arisen within the framework of civil law can be applied in public relations in almost the same form, effacing the boundary between public and private. This is a particular problem in Russia, where public law is often forced to "catch up" with private law.

Another example of the orientation of public law on private law is the domain of public services. By and large, the corresponding regulatory changes were introduced into the current legislation "proactively" without any serious scholarly support. We are referring to Article 7.3 of the Federal Law "On the provision of state and municipal services" of July 27, 2010, concerning the delivery of services in an anticipatory (proactive) manner. The normative text itself only gives schematic indications to state bodies to "carry out activities aimed at providing a service" that the applicant will need in the future. Even professional lawyers find it difficult to understand what this means exactly.

At the same time, this example shows how private law approaches can be borrowed to regulate the public sector on the basis of the idea of the free convertibility of personal data. In the digital economy, data about individuals (including their tastes, preferences, etc.) have already become a major source of profit for businesses. People, often without really understanding it, exercise the so-called "ownership" of data — the right to decide to whom, to what extent and for what remuneration to provide their data. This is the practice of social networking services, retail discount programs, etc.

Concerning the provision of proactive public services, personal data provided by citizens play a key role, even for future use. Nevertheless, no special regulations have been introduced so far, and such relations continue to be implemented outside the legal framework. In addition, there exist legal rules demanding the informed consent of an individual for processing his or her data. In the absence of clear regulatory procedures, there is a considerable risk of human rights violations in the process of providing proactive services, which is particularly unacceptable in the public sector

(in the private sector, the management of personal data still has alternatives due to free competition).

At the same time, on account of its mission of providing legal regulations in the sphere of digital technologies, digital law could solve the problem of striking a balance between public and private. The problem of assuring balance is familiar to courts: for example, the ECHR has developed principles for striking a balance between the right to freedom of expression and the right to respect for private life (questions such as "does the issue have public interest?" "is the individual a public figure and how well-known is he or she?" "what was his or her behavior before publication?" "what was the method of obtaining information and its reliability?" and "what was the form and consequences of the publication?" determine the severity of the imposed penalty).[1] In Russia, where the task of developing "ideal" legislation is still on the agenda, lawyers try to solve the problem of the balance of interests already at the stage of drafting normative texts that will subsequently be used by courts.

To a certain extent, the use of new legal structures could help to strike such a balance — for example, the right to informational self-determination as an adaptation of personal data protection to the conditions of big data processing. Nevertheless, despite its increasing popularity in Europe, especially in connection with the topic of profiling [Bosco F. et al., 2014: 28], the right to informational self-determination has not yet become popular in Russia and has not even been studied much.

It is also undeniable that digital law has very peculiar sources, including numerous self-regulatory acts and technical norms. It suffices to recall the international dream of regulating the Internet through an international convention (the ICANN organization, which continues to exist despite attacks), as well as the activities of international organizations in the digital sphere (such as the International Organization for Standardization, for example).

The foregoing discussion shows that, while digital law is still at an early stage of development, it has acquired a number of recognizable features.

2. Digital rights

If digital law is a branch of law, an institution or a discipline, then digital rights are the result of digitalization and should essentially be regulated

[1] Eur. Court H.R. Axel Springer AG v. Germany. Application no. 39954/08. Judgment of 07 February 2012; Eur. Court H.R. Von Hannover v. Germany. Applications nos. 40660/08 and 60641/08. Judgment of 07 February 2012.

by digital law. The penetration of digital technologies into the realization of almost all basic human rights has led to the emergence of new and specific rights connected with technologies and to discussions about the category of "digital rights."

Many researchers have written that the range of protected human rights will constantly expand. On the one hand, this should strengthen the legal protection of the individual. On the other hand, each "generation" brings with it a new logic of legitimizing claims called human rights, and conflicts of "new" and "old" rights are inevitable, which may ultimately lead to a poorer level of protection. Therefore, the following question arises: maybe it's better to have fewer yet better rights? [Busurmanov Z.D., 2010: 55].

At the same time, it seems that such minimization is no longer a priority in reality, and the new concept of digital rights is actively penetrating legal regulation. There are different ways of formulating digital rights, from analogies with classical rights to mixtures of different kinds. For example, the right to anonymity was formerly exercised by creative individuals who made products for public display or use. Today, the Internet has "granted" the right to anonymity to everyone, even not very creative individuals. Anti-libel protection and online defamation have led to a special combination and a new right — the right to be forgotten.

In legal doctrine, digital rights also include the right to the secure use of the Internet, the right to a virtual identity, and the right to use encryption [Levova I. et al., 2013: 41, 48], as well as the right to access the Internet and the right to be protected against unwanted information.

Since digital data are the primary building blocks of digital technologies, data security and legal protection have come to the fore. This means that the key element of the digital rights system is the right to the protection of personal data.

As one knows, European legislation on the protection of personal data has evolved gradually, theoretically "growing" out of the right to privacy. In European legal culture, the right to privacy is the basis for building relationships of citizens with the state and other people. With different legal nuances, this right is enshrined in the legislation of all European countries, sometimes at the constitutional level, and defended by courts.

Russian legislation in this area is pro-European in origin. Russia's European orientation in this area began with the ratification of the Convention for the Protection of Individuals. Furthermore, Federal Law no. 152-FZ "On Personal Data" of July 27, 2006, defined personal data in a broad sense (all

information relating directly or indirectly to a specific or identifiable individual), which is also fully consistent with the European approach. Most often, personal data includes the individual's surname, name and patronymic; year, month, day and place of birth; address; family, social and property status; education; profession; income; etc. New nuances arose with the spread of the Internet and the further digitalization of public relations, which made it easier to identify a person indirectly (for example, by comparing different data) without formally violating the rules of automatic data processing.

Finally, Federal Law no. 142-FZ of July 2, 2013, introduced Article 152.2 "Protection of a citizen's private life" into the Civil Code (unless otherwise provided by law, the collection, storage, distribution and use of any information about a citizen's private life is not allowed without his or her consent). To a certain extent, this has further strengthened the European approach to data protection as the protection of privacy.

At the same time, a broad definition of personal data that allows for different interpretations presents a problem for Russian law. Russian law enforcement always requires precise formulations at the level of the law in order to structure law enforcement activities uniformly. Whereas such broad definitions receive a judicial interpretation in Europe, they tend to be guided by the explanations of the competent executive body in Russia. The methodological recommendations of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) on processing personal data distinguishes three categories of personal data processed by operators:

personal data in general: all information related to the individual (name, date and place of birth, address, marital status, social status, etc.);

special categories of personal data (race, nationality, political views, religious or philosophical beliefs, health, personal life);

biometric personal data (information characterizing the physiological and biological characteristics of a person that can be used to establish his or her identity).

The concept of biometric data is not specified further, even at the level of executive directives. We only have the Roskomnadzor explanation "On the issues of referring photo and video images, fingerprint data and other information to biometric personal data and the specific nature of their processing" (2013), which, of course, cannot be considered to be normative. According to this memorandum, biometric personal data includes physi-

ological data (fingerprints, eye iris, DNA tests, height, weight, etc.) and other characteristics of a person that make it possible to establish his or her identity.

A full-fledged national system for the protection of personal data would require the establishment of an independent executive body responsible for monitoring compliance with legislation in this area. In Russia, these functions are (partially) performed by Roskomnadzor, which examines claims by citizens about the violation of their rights [Tereshchenko L.K., 2018]. To a certain extent, the protection of personal data is also within the competence of the Human Rights Commissioner of the Russian Federation. However, there is no special independent body in this domain in Russia.

Thus, Russian legislation in the field of privacy protection is, on the whole, guided by European standards. Nevertheless, it is recognized today that, in view of the growing digitalization of society, data protection standards need to be revised, since there is a clear contradiction between the requirements for protecting personal data and the actual impossibility of complying with them due to the proliferation of such data on the Internet. As scholars note, data depersonalization can no longer be an effective means of protecting personal data or, in a more general sense, the private life of citizens in the new technological reality [Saveliev A.I., 2015: 61].

At the same time, legislation on the protection of personal data can be used by the state for its own purposes. For example, Federal Law no. 242-FZ of July 21, 2014, requires operators that collect personal data, including through the Internet, to assure that the recording, systematization, accumulation, and storage of personal data of citizens of the Russian Federation takes place on databases located on the territory of the Russian Federation. At the same time, as scholars note, the consent of the citizens themselves to the cross-border transfer of their personal data is not taken into account, which contradicts Article 23 and Paragraph 4 of Article 29 of the Constitution of the Russian Federation [Ivanov A.A., 2015: 142].

In fairness, it should be said that Russia is not the only state that requires the personal data of its citizens to be localized on the territory of the country (similar legislation exists in China, Kazakhstan, Brazil, India, etc.). A fine is envisaged for violating this obligation (the maximum fine under Article 13.11 of the Code on Administrative Offenses of the Russian Federation is 75 thousand rubles); however, it is highly problematic to collect a fine from a foreign company that has no physical presence on the territory of the Russian Federation [Zherdina S., 2017: 5].

Another example of the state implementing administrative tasks at the expense of the personal data of its citizens is Federal Law no. 168-FZ "On the Unified Federal Register of the Population of the Russian Federation" of June 8, 2020. According to this act, information from the Federal Register is used to improve the provision of public services; implement state policy in the fields of socio-economic development, protection of citizens' rights, and national security; elaborate and implement state programs; draft budgets; and pursue other goals of state and municipal administration. Thus, the personal data of citizens serve the purposes of state administration, and the procedure of their use is entirely under the jurisdiction of the state.

Finally, there exist not only similarities but also differences between European and Russian data protection legislation. On the one hand, the balance between private and public interests in data protection and the protection of the state's interests is quite similar, especially after the series of terrorist attacks in Europe in 2010. On the other, the Russian state still prefers not to intrude too much into relations within the private sector, which is clearly a case of data protection in labor relations.

The Barbulescu case (ECHR judgment of September 5, 2017, on the case "Barbulescu v. Romania") drew sharp criticism in the West, as it was regarded as a complete ban on the use of employer's electronic means for personal purposes [Marquenaud J.-P., Mouly J., 2016: 1037]. Although the ECHR, referring to the Recommendation of the Committee of Ministers of the Council of Europe on the Processing of Personal Data in the Context of Employment, stated that employers should avoid unlawful and unjustified interference in employees' right to privacy, the court's task was to "clarify the nature and limits of the positive obligation of the state to protect the applicant's right to respect for his privacy and correspondence in the context of his employment." The court considered that the degree of control by the employer and the degree of interference with the employee's personal space should be separately assessed in each individual case. Here, a distinction must be made between monitoring the nature of the correspondence and its content. In addition, preference should be given to less aggressive methods and measures of penetration into an employee's personal life than directly viewing the content of his or her correspondence (for example, non-individual spot checks of data that are anonymous or have a generalized nature). In Russian legal doctrine, the fact that the ECHR considered the general ban on the personal use of the employer's technical means to be sufficient grounds to control the employee's personal communications in the course of disciplinary proceedings was regarded as "a step backward

in protecting employees' right to privacy" [Sychenko E.V., 2017]. Thus, the general assessment of the aforementioned ECHR judgment by researchers has been negative.

In Russia, an analogous dispute between an employee and his employer led to Decision of the Constitutional Court of the Russian Federation no. 25-P of October 26, 2017, on a case brought by A. Sushkov. His employer considered the fact that Sushkov forwarded information from the corporate email to his personal email address as the disclosure of confidential information. The courts judging the case also characterized the fact that Sushkov had sent emails containing the personal data of his colleagues through a mail server owned by Mail.ru LLC as the disclosure of confidential information. In support of this conclusion, the courts referred to the user agreement regulating the provision of e-mail services, under the terms of which the provider has the right to both restrict and allow access to information contained in users' e-mail boxes. According to the court, by virtue of Paragraph 5 of Article 2 of the Federal Law "On Information," this allows the e-mail provider to be recognized as the owner of confidential information posted by the plaintiff on an external e-mail address and, thus, points to the latter's disclosure of commercial information to a third party.

When considering the case, the Constitutional Court of the Russian Federation examined the user agreement and came to the conclusion that "its terms did not give the provider of the Internet service the right to authorize or restrict access to the information contained in the electronic messages transmitted by this service." When an individual sends to his (personal) e-mail address information that does not belong to him, he or she creates conditions for its further uncontrolled distribution. The legal consequences of such a situation vary depending on the reasonableness and discretion of the owner of the information. The rights of the owner of the information were violated by "the actions of the citizen who, contrary to the rules established by local and other legal acts (with which the citizen was familiar), transferred information from the corporate email address to his personal email address, if the owner of the information took all the necessary measures to prevent unauthorized access to this information by third parties."

In the opinion of Russian legal scholars, the Constitutional Court's decision encourages employers to introduce local regulations that would directly prohibit the transfer of information from a corporate email address to a personal address — these regulations *de facto* receive the force of federal law [Kiselev A., 2017]. A comparison of the European and Russian

cases shows that, on the one hand, the private law component prevails in relations between citizens and employers in Russia and, on the other, the Russian court, unlike the ECHR, did not raise the issue of the legality of checking the employee's personal mail at all.

Speaking about digital human rights, one cannot help but note a terminological inconsistency. In Russia, the term "digital rights" has been usurped by civil law. According to Federal Law no. 34-FZ of March 18, 2019, "Digital rights are obligations and other rights so characterized by law, whose content and conditions of application are determined by the rules of the information system that meets the characteristics established by law. The implementation, transfer and sale of digital rights, as well as their pledge and restriction of transfer, may only be performed by the information system itself without the involvement of any third parties." At the same time, the introduction of the term "digital rights" into the Civil Code was criticized by leading representatives of the civil law doctrine as an unnecessary redundancy, since these rights duplicate traditional law.

Such terminological inconsistency creates, at the very least, the risk of misunderstanding by foreign colleagues, theorists and practitioners. "Digital rights" are understood throughout the world in the context of human rights and public law. When it introduced this concept into its Civil Code, Russia came into contradiction with the continental legal system. There are two ways out of this predicament in our opinion. The first is to continue using the term "digital rights" in relation to digital human rights, always mentioning the context and keeping in mind that a different meaning of digital rights exists in civil law (with regard to its incomprehensibility for the global legal community, this resembles the situation of the "public agreement," which is understood as a retail trade agreement in the Civil Code of Russia). The second is to introduce a new term for the public law designation of digital rights — for example, "binary rights." This term would be quite apt, as it refers to the digital transmission of information ("binary") as well as to the notion of duality — the existence of rights both online and offline.

Conclusion

Summing up our brief polemical study, we should note that the interest in digital technologies keeps growing, and so the law needs to react quickly. The notion of "digital data" now appears directly in the text of the Russian Constitution (Art. 71), which significantly enhances the official status of digital law. Only a large-scale approach to digital law as a regulatory system and the utmost attention to the development of digital rights,

the implementation of which affects the direct interests of almost every citizen, will allow the state to maintain an appropriate level of regulation that does not impede technological development. At the same time, one should bear in mind that it is becoming increasingly difficult to strike a balance between public and private and between different human rights. Nevertheless, the neutrality and universality of technology gives hope that these problems can be solved in a uniform manner.

References

Blazheev V.V. et al. (2020) *Digital law*. Moscow: Prospekt, 640 p. (in Russian)

Bosco F., Creemers N., Ferraris V. et al. (2014) Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European data protection authorities. In: Reforming European Data Protection Law. P. de Hert (ed.). The Hague: Springer, pp. 3–33.

Busurmanov Zh. D.(2010) *The Euroazian concept of human rights.* Astana: University, 180 p. (in Russian)

Easterbrook F. (2012) Cyberspace and the law of the horse. Available at: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles (accessed: 20.04.2019)

Galuzo V.N., Kanafin N.A. (2018) Digital law in Russia: nonsense or reality? *Pravo i gosudarstvo,* no 8, pp. 118–125 (in Russian)

Golovkin R.B. et al. (2019) "Digital rights" *и* "digital law" in digitalization of economy and state rule. *Vestnik Vladimirskogo juridicheskogo instituta,* no 2, pp. 163–166 (in Russian)

Ivanov A.A. (2015) Personal data deposit abroad: a view of Russian law. *Zakon*, no 1, pp. 134–143 (in Russian)

Ioffe O.S., Shargorodskyi M.D. (1961) *Issues of legal theory.* Moscow: Juridicheskaya literatura, 381 p. (in Russian)

Kiselev A. (2017) Who owns information... *Trudovoe pravo*, no 12, pp. 93–101 (in Russian)

Lessig L. (1999) *Code and other laws of cyberspace.* N.Y.: Basic Books, 297 p.

Lessig L. (2011) The law of the horse: what Cyberlaw might teach. Available at: http://cyber.law.harvard.edu/works/lessig/finalhls.pdf. (accessed: 20.04.2020)

Levova I. et al. (2013) *Rights of Internet-users: Russia and world, theory and practice.* Moscow: Scholar, 143 p. (in Russian)

Marquenaud J.-P., Mouly J. (2016) Big boss is watching you. Alerte sur le contrôle des activités électroniques du salarié. *Revue trimestrielle des droits de l'homme*, no 108, pp. 1037–1048.

Rozhkova M.A. Digital law: what it means and how it is differed from cyber law? Available at: URL: https://zakon.ru/blog/2020/03/15/cifrovoe_pravo_digital_law_chto_eto_takoe_i_chem_ono_otlichaetsya_ot_kiberpravainternet-pravakompy (accessed: 11.01.2020) (in Russian)

Saveliev A.I. (2015) Implementing legislation on personal data in the era of Big Data. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* no 1, pp. 43–66 (in Russian)

Sychenko E.V. (2017) Practice of the European Court on Human Rights in the sphere of labour rights protection. *Precedents of the European Court of Human Rights,* no 1, pp. 4–13 (in Russian)

Tereschenko L.K. (2018) State control and personal data protection. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* no 4, pp. 142–161 (in Russian)

Tulikov A.V. (2016) Foreign legal thought in the era of IT. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* no 3, pp. 235–243 (in Russian)

Vasiliev A.A. et al. (2019) The term "digital law" in doctrine and legal texts. *Jurislingvistika*, no 11, pp. 15–18 (in Russian)

Yakovlev V.F., Talapina E.V. (2012) The role of public and private law in economic regulation. *Zhurnal rossiyskogo prava*, no 2, pp. 5–16 (in Russian)

Zherdina S. (2017) Localization of personal data on Russian persons for foreign companies. *Ezh-jurist*, no 4, p. 5 (in Russian)