ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

1/2021

Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

1/2021

ISSUED QUARTERLY

Articles

Comment

Book Review

Publisher
National Research
University Higher School
of Economics

Address:
3 Bolshoy Triohsviatitelsky Per., Moscow 109028, Russia
Tel.: +7 (495) 220-99-87
https://digitalawjournal.hse.ru/
e-mail: lawjournal@hse.ru

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)

Blockchain, Smart Contracts and Intellectual Property. Using distributed ledger technology to protect, license and enforce intellectual property rights

Ronny Hauck

Professor, Alexander Humboldt University. Address: 6 Unter den Linden, Berlin 10117, Germany. E-mail: ronny.hauck@rewi.hu-berlin.de

Abstract

For several years, almost everyone has been talking about blockchain. The underlying distributed ledger technology has become (in)famous as the technology behind cryptocurrencies such as Bitcoin and Ether. But what about blockchain and intellectual property like patents and copyright? Could this technology be used for the protection and enforcement of such rights? Which role can smart contracts play in this regard? This article focuses on questions concerning the requirements for provingthe protection of technical inventions as well as on the administration and exploitation of intellectual property rights. The latter could play an important role for intellectual property, which has not been registered or is not subject to registration, such as copyright. For trade secrets, a blockchain could be a useful tool for providing appropriate confidentiality measures. Last but not least, smart contracts in particular could be involved in connection with the transfer and, even more importantly, the licensing of intellectual property and mainly of software.

Keywords

blockchain, distributed ledger technology, smart contracts, intellectual property management, trade secrets, software, digital register, licensing, micropayment.

For citation: Hauck R. (2021) Blockchain, smart contracts and intellectual property. Using distributed ledger technology to protect, license and enforce intellectual property rights. *Legal Issues in the Digital Age,* no 1, pp. 17–41.

DOI: 10.17323/2713-2749.2021.1.17.41

1. Blockchain and smart contracts — technical background and challenges

1.1. Introduction

In its basic form, a blockchain[1] is an open ledger of information that can be used to record and track transactions and which is exchanged and verified on a peer-to-peer network [Clark B., 2018]. This paper analyzes use of blockchain technology in relation to intellectual property[2] with a specific focus on smart contracts. It is, however, not intended to examine questions regarding possible protection of the technologies concerned or of individual components or applications of intellectual property rights, for example to software or a database; see [Yanitsky-Ravid S., Kim E., 2019]; [Hoin-Hein N., Barth G., 2021]. Rather, it is a matter of working out what significance this technology already has or could have in the future — for example in dealing with patent-protected inventions or copyrighted works, as well as its significance for products developed on the basis of such intellectual property.

1.2. Blockchain/distributed ledger technology

Blockchain is the best known and most commonly used distributed ledger technology. Distributed ledger technology is a technology that facilitates an expanding, chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. The concept of blockchain was first introduced to the public in October 2008 by a person (or group of persons) who published a paper under the pseudonym "Satoshi Nakamoto" entitled "Bitcoin: A Peer-to-Peer Electronic CashSystem" [Ross E., 2017: 359–360].[3] A blockchain can be understood as a decentralized, i.e. distributed database. It has no central server and thus no central authority that checks and verifies the transactions. From a business point of view, a blockchain is an exchange network

[1] For technical background of blockchain see [Pilkington M., 2016]; [Allessie D., 2019].

[2] For the purposes of this article, the term includes trade secrets. In German law, for example, most academics do not consider trade secrets (*Geschäftsgeheimnisse*) as an intellectual property *right (Immaterialgüterrecht)*, but nevertheless as a type of intellectual property (*Geistiges Eigentum*). Unless otherwise noted, this article is limited to questions of European and German law.

[3] Available at: https://bitcoin.org/bitcoin.pdf (accessed: 24 Feb 2021). Since then Blockchain has developed from version 1.0 to version 3.0. Blockchain 1.0 emphasizes virtual currency, but with Blockchain 2.0 the values being transferred are programmable transactions in the form of smart contracts. Blockchain 3.0 represents the expansion of the technological applications beyond finance and markets.

for moving value between peers, who themselves are functional units in the same layer of a network.

Different types of data can be added to a blockchain, from cryptocurrency (most notably Bitcoin and Ether — ETH) and transactional and contractual information to data files, photos, videos and contract documents. While Bitcoin was designed as a cryptocurrency, several blockchains have been created since then for different purposes and every one of them contains distinctive features Gurkaynak G., 2018: 848]. For example, the Etherum blockchain is a "Turing complete blockchain" [Sergey I., 2018] with the ability to run smart contracts (see below 1.3).

The respective data is written into a "block" as soon as it has reached a certain capacity. This process repeats continuously until the next block is filled. Each block refers back to the previous one, so that a chain of blocks — called a "blockchain" — is created. This leads to a distributed and highly redundant[4] "data archive", which makes it impossible to delete the data. The blockchain is immutable;[5] blockchain records are time-stamped and traceable. Therefore, the real innovation of distributed ledger technology is that it ensures the integrity of the ledger by means of crowdsourcing supervision and removes the need for a central authority, e.g. public registries. In other words, transactions are verified and validated by the multiple computers that host the blockchain (the so-called nodes). For this reason, it is seen as "nearly unhackable," because a cyber-attack would have to strike out (nearly) all copies of the ledger simultaneously in order to change any of the information on it [Clark B., 2018]. In summary, the main features of blockchain technology are data integrity, verification and public transparency of transactions [Allessie D., 2019].

The term "hashing" is also particularly important, as hashes are the central security element in a blockchain. A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic hash function is characterized by its extreme difficulty to revert, i.e. the recreation ofthe input data solely from its hash value [Pilkington M., 2016]. This sequence of letters and numbers is a kind

[4] Data redundancy: a condition created within a database or piece of data storage technology in which the same piece of data is held in separate places. Available at: https://www.techopedia.com/definition/18707/data-redundancy (accessed: 24 Feb 2021)

[5] However, some scholars dispute whether the term "immutable" accurately reflects nature of the blockchain; a definition of the concept of "immutability" as it relates to the blockchain, aligns with the term "unchangeable" [Walch A., 2017: 736–739].

of unique digital fingerprint, which is always unique for each different data set [Kuchta R., 2017]. As a result, hashing is used for the verification/validation process of the blockchain, which takes place through so-called "mining" (the creation of a new block).

The blockchain is therefore a procedure in which the falsification and deletion of the content concerned is precluded by the cryptographic encoding of chained entries. This opens up the possibility of tracing economically significant transactions — such as the transfer or licensing of IP — in a tamper-proof manner. Furthermore, actions against counterfeiting in particular could play an important role in the present subject.

1.3. Smart contracts

As mentioned above, using the Etherum blockchain as an example, smart contracts are a mechanism for expressing computations on a blockchain. A single, generally accepted definition of the term "smart contracts" does not exist. According to one widespread view, a smart contract is a program that is stored in a tamper-evident and tamper-proof manner and is guaranteed to execute upon the fulfilment of certain predefined criteria [Szabo N., 1997]; [Raskin M., 2017]. In particular, the program code allows digital assets or representations of physical objects to be reallocated in the form of transactions between two or more parties on the basis of other (external) data not yet known at the time the code was programmed. More generally, such software could also be described as controlling, monitoring and/or documenting legally relevant actions (in particular an actual exchange of services) as a function of digitally verifiable events[6].

As a "computerized transaction protocol that executes the terms of a contract" [Tapskott D., Tapskott A., 2016: 72, 83, 101, 127], smart contracts are a conceivable field of application of the blockchain technology. The idea behind these "intelligent contracts" is — to put it simply — that the contracts can ultimately execute themselves and sometimes act autonomously. Thus, smart contracts allow the performance of transactions without the involvement of third parties. The transactions are traceable and irreversible. One possible example is the granting of usage rights (licenses) for actions with copyright implications on the internet and in particular, the resale of such

[6] However, smart contracts are not "smart" in the sense of (strong) AI, as they are unable to understand natural language or to independently verify whether an event has occurred which is relevant for execution of the smart contract. They also cannot be qualified as "contracts" in the legal sense because they are (just) a computer-programmable ´if/then´relation and are incapable of taking wider contextual factors into account.

rights (see below 4.3). Another field of use of blockchain technology could be the creation of a system for near-real-time payments for public performances of musical works. Thereby, music licensing could be implemented through smart contracts [McJohn S., McJohn I., 2016: 10, 11].

1.4. Challenges

In general, from a technical point of view, the main challenge prohibiting the widespread adoption of distributed ledger technology for the management of IP rights is the difficulty of explaining and understanding the complexities of the technology itself. Therefore, only applications with simple and easy-to-use interfaces are likely to be accepted and used in the (near) future [Gurkaynak G., 2018: 860, 861].

Furthermore, there are also very specific technical challenges could prevent the technology from being widely used. For example, when using a blockchain for transactions and, in particular, as a (micro-)payment system, a significant technical problem currently facing blockchain technology is the speed with which the respective transactions can be processed, as blockchain is significantly slower than traditional transaction platforms such as VISA or PayPal.[7] In addition, since the users of a blockchain system are also the nodes of the system in a blockchain, each user would need to store massive amounts of data. Despite these concerns, given the rapid technical developments in storage technology in recent years, one can nevertheless hope that software developers will resolve this issue in the near future.[8]

Blockchain technology faces several legal challenges, too. Firstly, it is often difficult to determine which jurisdictions' laws and regulations apply to a given blockchain application, as the nodes of a decentralized ledger can span multiple locations around the world, resulting in an overwhelming number of laws and regulations which could apply to transactions in a blockchain based system [Salmon J., Myers G., 2019]; [O'Shields R., 2017: 190]. Regarding smart contracts in particular, if there is ambiguity as to the location where the contract was concluded, the courts will have to find a method of defining and determining the place of conclusion of the smart contract [Fulmer N., 2019: 185–186]. In addition, the fa.ct that smart contracts do not necessarily require legal enforcement may make them attractive for illegal transactions. Therefore, legal challenges could provide a considerable obstacle to development and widespread adoption of services based on distributed ledger technology.

[7] Ibid, p. 850.

[8] Ibid., p. 861.

2. Protection of technical inventions and trade secrets

2.1. Technical inventions

Technical inventions are (primarily[9]) protected by patents. Article 52(1) of the European Patent Convention (EPC) states that

European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

Consequently, both novelty and the "inventive step" (better defined as "non-obviousness") [Sai Deepak J., 2010: 410–427]; [Lauber-Ronsberg A., Hetmank S., 2019] are prerequisites for patentability.[10] Article 56 EPC states that an invention shall be considered as involving an inventive step if, having regard to the state of the art, it is not obvious to a person skilled in the art. The invention shall be considered to be new if it does not form part of the state of the art (Article 53(1) EPC).

Decisive importance is therefore attached to the "state of the art". This includes "everything made available to the public by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application" (Article 54(2) EPC). As this broad wording suggests, the greatest challenge in examining the patentability of an invention is to determine the state of the art and thus to identify all information in the meaning of Article 54(2) EPC. It is not only the status quo in the country of filing that is significant, but also all the publicly available information (the relevant specialist knowledge) worldwide in the field relevant to the technology being applied for a patent. There is no territorial restriction with regard to the publicly available state of the art.

This also applies in US patent law, where — similar to European law — novelty and prior art are also prerequisites of granting patent protection. A patent will not be granted for a technical invention if information about the patented product or process (or the underlying technical solution) was publicly available and thus known before the relevant priority date of the patent, since 35 U.S.C. 102(a) states as follows:

[9] Under German law, technical inventions are also protectable as utility models (*Gebrauchsmuster*).

[10] The requirement to be "susceptible of industrial application" is of least importance since an "invention shall be considered as susceptible of industrial application if it can be made or used in any kind of industry, including agriculture" (see Article 57 EPC), a requirement which is usually easy to fulfil.

A person shall be entitled to a patent unless—(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention […].

There is also no territorial restriction in US law with regard to information harmful to novelty. The only decisive factor is the accessibility of the relevant information to the public.[11]

As each block of a blockchain contains not only a cryptographic hash of the previous block, but also a timestamp, one conceivable field of application for blockchain technology could therefore be the documentation of the innovation process — the inventive steps that ultimately led to the technical invention worthy of protection. The evidential function of a blockchain could be used in technical developments (which are to be patented as inventions), for example, to document the development cycle of a product and thus the state of the art, or the further development of the product achieved by the invention in question, without gaps — and in a tamper-proof manner.

2.2. Actions against patents

The function of a blockchain as described above (e.g. the documentation of the invention process) could also be used *vice versa* against patents which have already been granted. There are several ways of limiting the scope of the patent or even invalidating a patent (revocation). Under the EPC (see Article 100), an objection can be filed "on the grounds that the subject-matter of the patent is not patentable under Articles 52 to 57", which includes the requirements of "novelty" and an "inventive step"(non-obviousness, see above 2.1). For example, it could be argued against the patent of a third party (and in particular that of a competitor) that a technical solution already belongs to the state of the art, i.e. is not new and does not constitute an inventive step. Based on such information, precisely because of the strong evidentiary function of the information stored in the blockchain, the patent in question could be declared invalid (in whole or in part). It could also be easier for the defendant to prove in a patent infringement process the invalidity of a patent, meaning that it could not be infringed at all. Because, if the defendant files an action for nullity against the patent, the court that decides on the patent infringement (*Landgericht*)

[11] See e.g. In re Wyer, 655 F.2d 221, 226, 210 USPQ 790, 794 (CCPA 1981) (regarding an Australian patent application).

might be more inclined to use this information to initiate the infringement process in accordance with Section 148 of the Code of Civil Procedure in order to wait for the outcome of the nullity proceedings before the Federal Patent Court (the so-called injunction gap).

So far, German courts have been generally reluctant to stay proceedings solely because of parallel pending proceedings on oppositions or nullity. They will only do so if the defendant provides sufficient evidence and arguments to convince the court that there is a substantial likelihood of the patent being invalidated. In a patent infringement lawsuit, the blockchain — or the information stored there — can thus have the function of a both a shield and a sword.

2.3. Co-inventors and R&D-cooperations

As many technical solutions are developed in a team,[12] a tamper-proof blockchain can also be used to prove the exact involvement of individuals in an invention process. This becomes even more complicated if such a team does not consist solely of employees of one company, but also of external persons, for example within the framework of a research and development (R&D) cooperation or even an open innovation process. In practice, the question of who actually participated in the development and to what extent is not always easy to answer. On the one hand, it is often not fully documented who was involved in the invention process at all. On the other hand, it is also not particularly easy to determine, especially when the cooperation has ended, how large the contribution of the participants to the invention actually was.

In R&D cooperations and irrespective of the situation of the co-inventors just described, the aforementioned documentary function of the blockchain can also become important, since it could be established beyond doubt which cooperation partner has made which developments and when. This can considerably facilitate the later assignment of the respective intellectual property developed during the cooperation, the so-called "foreground-IP". In addition, license agreements can be managed within the framework of smart contracts (for licensing of IP through smart contracts see below 4.2), for example with regard to the background-IP of the

[12] In German law, if several people are involved in an invention, they form an inventor community (*Erfindergemeinschaft*). The co-inventors share the right to the invention in accordance with Sec. 6 second sentence of the Patent Act. The relevant law, however, can only be found in the German Civil Code, Sec. 741–758.

parties involved or the later exploitation of the cooperation results [Hohn-Hein N., Barth G., 2018: 1094].

2.4. Protection of trade secrets

It is safe to say that during the process of searching for a technical solution to a technical problem, which, if successful, leads to a patentable invention, extensive technical knowledge (know-how) is created, which does not necessarily flow fully into the invention. In cooperations, such know-how becomes part of the foreground-IP. For companies, however, such knowledge can be just as important and in some cases even more valuable than the patent-protected invention itself. When dealing with trade secrets, it has long been discussed whether trade secrets can be seen as a type of (intellectual) property. This discussion cannot be continued here. It is, however, generally recognized that the essential elements of trade secret protection are confidentiality and (limited) access. Therefore, the person who actually controls the access to the information concerned can be considered its "owner" or "holder".

Given the specifics of the distributed ledger technology (see above 1.2), the blockchain could serve to prove the source of this knowledge and who is actually entitled to this know-how. Additionally, the blockchain could play a role in the protection of trade secrets. Information (know-how) not protected by a patent may nonetheless fall under general concept of a "trade secret" pursuant to Directive 2016/943 (the Trade Secrets Directive) and is only of value to the holder[13] if it is not generally known. In accordance with the requirements of Article 2(1) (a) of Directive 2016/943, only information that

> "is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question"

is protected as a trade secret. This requirement is based on Article 39(2) (a) TRIPS:

> "[such information] is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; not generally known or readily ascertainable".

[13] According to Article 2(2) of Directive 2016/943 "'trade secret holder' means any natural or legal person lawfully controlling a trade secret".

The "holder" must therefore ensure that the information in question[14] does not become public knowledge. This applies accordingly to non-technical information (in particular commercial knowledge such as information about customers, prices, etc.) that can easily have (at least) a similarly high value for a company.

In addition, the holder of such trade secrets can only take civil action against infringers if they can prove that the respective information "has been subject to reasonable steps under the circumstances" to keep the information secret (Article 2(1) (c) Directive 2016/943). The term "reasonable steps" still needs judicial interpretation. This is comparable to US law, where "reasonable efforts" or "reasonable measures" must be proven (cf. Section 1(4) (ii) Uniform Trade Secrets Act and 18 USC Section 1839 (3) (A) Defend Trade Secrets Act respectively).

How valuable the information in question is for the holder or — from a different perspective — what negative consequences disclosure would actually have depends on the individual case. It can be assumed, however, that the more valuable the information is, the higher the requirements will be for "reasonable steps" to keep it secret. Nevertheless, for the adequacy of the measures to keep the respective information secret, the specific (financial) capabilities of the respective company of ensuring effective protection of secrets must also be taken into account. In principle, large companies have better personal and technical resources than small and medium-sized enterprises (SMEs). As a result, the latter are likely to face challenges under the new law, although it should be noted that the Directive pursues the goal of promoting SMEs (see Recital 2 Directive 2016/943). However, this will hardly be possible if the actual feasibility and thus the reasonableness of the measures are not taken into account for SMEs, as otherwise the Directive would ultimately have a negative effect on the protection of trade secrets in the European Union's internal market.

The limited access to the relevant information (the respective trade secret) is made possible by the hash mentioned above (see above 1.2) as the actual security mechanism. Therefore, as a rule, no access restrictions to the blockchain system are necessary ("permissionless" or "public" blockchain[15]). However, the problem with the protection of secrets *by* the block-

[14] According to Article 2(1)(b) of Directive 2016/943, the information has to have "commercial value because it is secret".

[15] As members of the blockchain network are free to negotiate the level of decentralization that the network will have, partially decentralized blockchains are also possible (semi-permissioned blockchain).

chain lies in the fact that the technology is based on a decentralized and ultimately transparent architecture, which may not be compatible with the idea of the protection of trade secrets at all. Protection of trade secrets could therefore only be considered as appropriate if the relevant information is not itself stored, but only the hash. The owner of the unchanged file could then reproduce this hash using an encryption program and prove the sole ownership of the information.

Due to the comprehensive protection against falsification and deletion of information, as well as the possibility to regulate access to it, the blockchain could therefore play an important role in the protection of trade secrets. In addition, the blockchain's function in this respect — to provide evidence that the information has been "subject to reasonable steps […] to keep it secret" — also provides proof of who actually controls the non-public information and is therefore the "holder" (pursuant to Article 2(2) Directive 2016/943).

Furthermore, it is conceivable not to use a public system (a permissionless blockchain), but instead to employ a system with restricted access, a "private" — or "permissioned" — blockchain, even if this contradicts the original idea of transparent data and information storage. The idea of the blockchain as distributed ledger technology was originally to create transparency by distributing the data records across a network (on a large number of computers), thus protecting the data from falsification, destruction and suppression [Blocher W., 2017: 338]. While the traditional concept of blockchain is an open and anonymous network, there are also "private" blockchains, which pre-screen who is allowed to administer the ledger. Permissioned blockchains act, in contrast to public blockchains, as closed ecosystems, where users are not freely able to join the network, to see the recorded history, or to carry out their own transactions [Dob D., 2018]. Such blockchains are run by specific members of consortiums or companies on a private network (intranet or VPN) [Finck M., 2019: 14,15] and members need to opt-in to the creation of such a network. Additionally, only approved people or computer entities are able to run nodes on the network, validate transaction blocks, issue transactions, execute smart contracts, or read the transaction history.

With regard to trade secrets, a "proof of participation" mechanism must be used to prove special entitlement to participate in the system. It will usually be prudent for the holder of the trade secret to grant the corresponding authorisation solely to trustworthy persons as a central point of legitimation. This limitation of access is therefore the first stage of the "reasonable

steps" to keep the information secret, which must be proven in accordance with the provisions of the Directive as desribed above. The evidential value of information stored in such an architecture will, of course, be lower than that of a blockchain with a "genuine" distributed ledger approach.

3. Copyright

In contrast to patent law — patent protection requires that the patent has been granted and published in the patent register — and according to Article 2(2) Berne Convention ("The enjoyment and the exercise of these rights shall not be subject to any formality"), copyright protection for works of art does not arise through a constitutive official act, but solely through the fact that the work in question is created.

In German law, even declaratory registration is not necessary, nor is it possible, as such a register does not exist. In contrary, until the USA joined the Berne Convention in 1989, all works had to be registered in the USPTO's Copyright Register in order to be protected by copyright, meaning the registration was therefore constitutive. Since then, protection in the USA also arises with the creation of a work, but in order to conduct an infringement suit, it is still necessary to register a work created in the USA by a US citizen in the Copyright Register (see Section 411(a) of the Copyright Act).

As a general rule, the copyright holder is the person who created the work (the author). The author must provide proof of actual authorship of a particular work. As already described above in relation to technical inventions, the blockchain could have a documentary function if the process of the creation of a copyrighted work is recorded there [Hohn-Hein N., Barth G., 1092]. Not only would this allow documentation of the ownership of the rights, but also the comprehensible recording of the actual scope of protection for the work, described in detail. The blockchain would thus become a digital register, whereby the entries would have a purely declaratory character.[16] However, such registrations are likely to be far more significant than described above in relation to copyrighted works at their exploitation stage. Registrations of this nature could be even more significant

[16] Platforms like binded.com ("the world's first copyright platform") are based on distributed ledger technology. Authors can upload their copyrighted works (most notably photographs); Binded creates a digital fingerprint of it and writes a permanent record into the bitcoin blockchain. It also provides a "copyright certificate" to prove the ownership of the respective person.

and important for the purposes of documenting the granting and scope of rights to exploit copyrighted works (see below 4).

As already mentioned in relation to technical inventions, the situation in which several people collaborate to create a copyrighted work can be a source of conflict. For example, think of a computer program created by several software developers. In this respect, too, copyright protection is available to all developers collectively. The resulting problems can then be similar to those of the inventor community (see above 2.3). In this case, the storage of information about the creative process in a blockchain could also have the function of documenting the actual contribution of the individual co-authors to the work (the computer program) with high accuracy.

4. Transfer and licensing of intellectual property

4.1. Blockchain as a digital register

A blockchain peer-to-peer network could be used to enable the tamper-proof and erasure-proof recording of transaction histories, such as during the transfer and licensing of intellectual property rights. The intervention of a third (neutral) authority — a private or state intermediary — would then become obsolete [Gurkaynak G., 2018: 855]; [Schrey J., Talhofer T., 2017: 1431]. The blockchain could thus have the function of a digital and trustworthy register, especially in the case of intellectual property rights and/or licenses of such rights for which such a register does not exist, namely in copyright law and more generally for the documentation of sales and licensing transactions.

4.2. Technical IP — transfer, licensing and insolvency procedures

The patent owner or the exclusive licensee can assert claims arising from the patent in their own name, especially in the case of a (presumed) infringement. Therefore, the plaintiff must prove that they are actually the holder of the relevant patent (or at least that they hold an exclusive license). This can be difficult in cases when the patent was aquired from the original owner, because patents are not necessarily sold individually. Instead, entire patent families or even patent portfolios which can consist of a very large number of patents (and patent applications) are often transferred. Furthermore, the assignment of patents is free of any form requirement; in particular, no change to the patent register is required to make the acqui-

sition effective.[17] The relevant change in the register to be requested from the patent office is nevertheless important because the patent register has a presumptive effect with regard to patent ownership.[18] In European law, Rule 22 *et seq*. of the "Implementing Regulations to the Convention on the Grant of European Patents" state that the transfer of a European patent application can be recorded in the European Patent Register. These applies *mutatis mutandis* to the grant or transfer of a license, the establishment or transfer of a right *in rem* in respect of a European patent application and any legal means of execution affecting such an application.

Especially in the case of cross-border patent transfers, commonly there is a failure to document the transfer history and to update the patent register. This can cause significant problems as, before German courts, the plaintiff has to prove in an infringement proceeding that they actually are the holder of the patent which is the subject of the suit, especially if the defendant denies this ownership. Otherwise, the claim will most likely be dismissed as inadmissible owing to a lack of standing (*Prozessführungsbefugnis*).[19] For these purposes, the use of blockchain technology conveniently provides the ability to document such transfers.[20]

Regardless of any impending or ongoing infringement dispute, companies may need to prove that they actually own certain patents. This applies, for example, to start-ups because it can be important for investors to have complete evidence of the actual ownership of patents and patent applications which are crucial to the companys business and therefore essential for the valuation of the company. This function — the proof of ownership by blockchain — applies in a comparable way to corporate transactions, for example in the context of due diligence to determine which intellectual property rights and licenses the company in question actually has.

The question of ownership of patents and patent licenses can also play an important role in the insolvency of a company. Accordingly, in indi-

---

[17] As an exception, an assignment of a European patent application "shall be made in writing and shall require the signature of the parties to the contract" (Article 72 EPC).

[18] In German patent law, the Federal Supreme Court uses registration as an important indicator of ownership, see Judgement of the Court, 7 May 2013 — X ZR 69/11, 197 BGHZ 196 — Fräsverfahren.

[19] Another view is that the lawsuit would be unfounded because of a lack of ownership (*Aktivlegitimation*).

[20] DLT-based platforms already exist on which intellectual property rights can be traded. The platform LEXIT (www.lexit.com) describes itself as "the first M&A marketplace where anyone can buy and sell IP, code, tech, and companies, via an all-in-one platform powered by blockchain".

vidual cases it may be crucial whether a company actually holds a patent or at least an exclusive license. This is because a simple license would not be protected if the licensor were to become insolvent. As permitted by German law, the insolvency administrator could be inclined to terminate the license agreement and thus eliminate the legal basis of the license, according to the Insolvency Statute, Sec. 103:

(1) If a mutual contract was not or not completely performed by the debtor and its other party at the date when the insolvency proceedings were opened, the insolvency administrator may perform such contract replacing the debtor and claim the other party's consideration.

(2) If the administrator refuses to perform such contract, the other party shall be entitled to its claims for non-performance only as an insolvency creditor. If the other party requires the administrator to opt for performance or non-performance, the administrator shall state his intention to claim performance without negligent delay. If the administrator does not give his statement, he may no longer insist on performance.

The (former) licensee could then no longer invoke a right of use, which could have a significant negative impact on their activities. If, on the other hand, they are the owner of the patent — resulting from a transfer and not a mere licensing of the patent, which can be easily demonstrated through the blockchain — or they are at least the owner of an exclusive license, their legal status would be secure [Pahlow L., 2017: 140]; [Zurth P., 2020: 25].

4.3. Software licenses in the era of "UsedSoft"

As already was noted by Alexander and Peter Hoppen [Hoppen A., Hoppen P., 2018], one highly relevant application of the blockchain is the management of software licenses based on the ECJ´s decision "UsedSoft/ Oracle" from 2012[21] and subsequent decisions of national courts.[22] In that particular case, the plaintiff (Oracle) had developed client-server software, which was sold primarily to commercial customers, mostly together with package licenses for at least 25 users. The license agreement granted the purchaser *inter alia* an unlimited (non-exclusive) non-assignable right to use the respective software. The software itself was not sold on a disk or

[21] Judgment of the Court (Grand Chamber), 3 July 2012, Case C-128/11, ECLI: EU:C:2012:407, UsedSoft GmbH v Oracle International Corp.

[22] See e.g. Federal Supreme Court, 17 July 2013 — I ZR 129/08, GRUR 2014, 264 — UsedSoft II; Federal Supreme Court, 19 March 2015 — I ZR 4/14, GRUR 2015, 772 — Green-IT.

another carrier, but was located on a central server. The (non-exclusive[23] and non-transferable) user right to such a program, which is granted by a license agreement for an unlimited period, includes the right to store a copy of the program permanently on a server and to allow a certain number of users to access it by downloading it to the main memory of their work-station computers. An additional maintenance agreement permitted the download of updated versions of the software (updates) and programs for correcting faults (patches) from Oracle's website.

The defendant — the company with the telling name "UsedSoft" — sold "used software licenses" by acquiring "unneeded" licenses to certain software (including the license keys) from the initial purchaser and reselling them. According to UsedSoft, their customers ("second-hand buyers") lawfully acquired the right to download the software directly from the website of the respective manufacturer.

Oracle, as the proprietor of the exclusive user rights under copyright law to those programs, considered the actions of UsedSoft and its customers as an infringement of Oracle's exclusive right of permanent or temporary reproduction of computer programs within the meaning of Article 4(1) (a) of Directive 2009/24 (the so-called Software-Directive). The defendant (UsedSoft) argued that the right to distribute the software had been exhausted, based on Article 4(2) Directive 2009/24:

> The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

Therefore, Oracle's customers were entitled to transfer the right of reproduction to the respective programs to third parties — an argument which the ECJ ultimately followed. The Court thus extended the scope of the principle of exhaustion (the so-called 'first-sale doctrine') to encompass software and software licenses, going far beyond the traditional understanding of this principle [Hilty R., 2018: 865].[24] However, in order to

[23] In addition, Oracle's license agreements state that the right to use the programs is "non-transferable".

[24] There has been a long debate about whether the ECJ's broad interpretation of the exhaustion principle/the first-sale doctrine in UsedSoft/Oracle also applies to other digital goods, like eBooks. On the basis of a recent decision of the ECJ, this should be answered in the negative, see Judgment of the Court (Grand Chamber), 19 December 2019, Case C-263/18, ECLI:EU:C:2019:1111, Nederlands Uitgeversverbond and Groep Algemene Uitgevers v Tom Kabinet Internet BV and Others.

solve the problem of the — theoretically conceivable — endless number of copying processes and program copies[25], the ECJ required the first purchaser to make "their" program copy unusable after resale.[26]

It is precisely in this regard — assuming the admissibility of this business model based on the ECJ's assessment — that the blockchain could have an important (evidentiary) function. This could be documented, in particular, by rendering the so-called first copy unusable on the part of the reseller (first buyer). This would put an end to the multiple use [Chohan U., 2017] of the software as required by the ECJ and, in wake of this decision, also by the German Federal Court, which places extremely high demands on such evidence.[27] As blockchain records are immutable and cryptographically secure, there would not be any reason for courts or other authorities to disallow or reject a blockchain record as proof [Gurkaynak G., 2018: 854]. The assignment of a license to an authorized person can be verified by presenting a certificate together with the transaction history, which is verifiable in the blockchain. The respective person, who may have to prove their authorization, has the necessary key for this.

Regardless of the "UsedSoft" situation, the blockchain could play an important role in other aspects of copyright contract law. Similarly to the aforementioned situation for patent licenses (see above 4.2), the proof that a license has actually been granted as well as the scope of that license (and thus compliance with the license conditions, see below 4.4) could be evidenced. In addition, any sublicensing with the creation of a so-called 'license chain' and the further transfer of copyright licenses could be documented by the blockchain as a digital register that is tamper-proof, so that anyone who has to prove their original or derived usage right at a certain point in time would be able to do so [Blocher W., 2017: 339, 340]; [Hohn-Hein N., Barth G., 2018: 1093].

4.4. Scope of IP licenses

With smart contracts, the contractually agreed services and further conditions are recorded using one piece of software. It is not actually a contract, but rather an illustration of one [Kaulartz M., Heckman J., 2016: 618,

[25] Of course, contrary to what the ECJ obviously assumes, a program copy cannot be transferred (and therefore resold). Rather, new copies are made and the reseller sells and transfers the issued licenses via "Used Soft".

[26] Judgment of the Court (Grand Chamber) 3 July 2012, Case C-128/11, ECLI:EU:C:2012:407, UsedSoft GmbH v Oracle International Corp, mn. 78.

[27] See Federal Supreme Court, 17 July 2013 — I ZR 129/08, GRUR 2014, 264 — UsedSoft II: Even a notarial certificate is not sufficient.

621]. The software in question can automatically use blockchain technology to check whether a contracting party has actually performed the owed service. The main function of the underlying technology in smart contracts is to document the obligations to be performed in a verifiable manner and ultimately to monitor their fulfillment. In the very paper where Nicholas Szabo coined the term "smart contracts", he suggested that one application of smart contracts would be to automatically disable a car if the loan payments were not made in timely fashion [Szabo N., 2019].

A license agreement on intellectual property rights can also be designed as a smart contract. In this respect, the underlying software could monitor whether e.g. the licensed patented technology or copyrighted software is only actually used to the extent contractually agreed. Therefore, the licensor could easily prove to the licensee any breaches of contract, which, pursuant to German law, are also violations of the intellectual property right itself.[28] It is also conceivable that the contract will be performed in such a case, for example in the sense that the licensee will no longer granted access to the software in the cloud by the licensor or that at least a corresponding warning is automatically issued. The payment of the license fees could also be processed via blockchain (see below 4.5).

4.5. Equitable remuneration for authors

Another area of application for blockchain technology is micropayment through digital currencies. The right to an equitable remuneration (*angemessene Vergütung*) for the use of the author´s work is one of the main tenets of German copyright law. Copyright Act, Sec. 11 states*:*

> Copyright protects the author in his intellectual and personal relationships to the work and in respect of the use of the work. It shall also serve to ensure equitable remuneration for the use of the work. (emphasis added)

This principle also forms the basis for Copyright Act, Sec. 32:

(1)The author shall have a right to the contractually agreed remuneration for the granting of rights of use and permission to use the work. If the amount of the remuneration has not been determined, equitable remuneration shall be deemed to have been agreed. If the agreed remuneration is not equitable, the author may require the other party to consent to a modification of the agreement so that the author is granted equitable remuneration.

[28] See Patent Act, Sec. 15(2)(1) and Trade Mark Act, Sec. 30(2). Although there is no such rule layed down in the German Copyright Act, the principle is also applicable to copyright licenses.

(2)Remuneration shall be equitable if determined in accordance with a joint remuneration agreement (section 36). Any other remuneration shall be equitable if at the time the agreement is concluded, it corresponds to what in business relations is customary and fair, given the nature and extent of the possibility of use granted, in particular the duration, frequency, extent and time of use, and considering all circumstances. […].

It is conceivable that remuneration for copyright-related usage could be processed via internet. This means that license agreements would not only be concluded automatically on a mass basis, but that the remuneration would also be processed at the same time — which is exactly what bitcoins were invented for [Nakamoto S., 2008].[29] The advantage is that the payment is actually case-dependent and usage-related and takes place directly between the user and the rights holder. This is a counter-model to the European and notably German system of copyright limitations[30] with lump-sum remuneration stipulated in framework agreements, which in turn can only be claimed by the collecting societies concerned.[31] Only in a further step, through the distribution, does the rights holder receive their remuneration. In a developed system of smart contracts, the standardization of the statutory limitations to the author´s rights could therefore be dispensed with, at least for private use. Any act of use would, first of all, have copyright implications and a license agreement in the form of a smart contract would be required (unless the right holder were to grant a gratuitous license). In return, the user would pay for the use, which would also be automated. This would make the entire collecting societies system — at least in this respect — obsolete.

Alternatively, collection societies can work with other companies to provide better service to their rights holders in an increasingly competitive

[29] The problem now, however, is that Bitcoin payment fees have risen sharply recently. Available at: https://bitcoinmagazine.com/articles/bitcoin-now-useless-micropayments-solutions-are-coming1/ (accessed: 24 Feb 2021). Therefore, Bitcoins can hardly be considered an inexpensive alternative, particularly to credit card payments.

[30] See Article 5 (Exeptions and limitations) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. In German law, the limitations of the author´s rights can be found in Chapter 6 (Limitations on copyright through lawfully permitted uses; section 44a et. seq.) of the Act on Copyright and Related Rights.

[31] In German law, collecting societies like GEMA and VG Wort are private, incorporated associations of authors, musicians, publishing houses etc. with the aim of common enforcement of copyrights. Their function is the administration of the rightholder's fee from secondary usage rights (right of reproduction, right of distribution etc.). The general legal priciples are enshrined in the Law on Collective Rights Mangement (Verwertungsgesellschaftengesetz); see also Reinbothe (2015).

market for collecting societies in the EU.[32] An example for using distributed ledger technology in this way is the music blockchain startup Revelator, working with the music recognition service BMAT and the Finnish music collecting society Teosto. The application "Artist Wallet" enables the payment of performance royalties to composers for radio airplay. BMAT runs a music recognition service that uses fingerprinting technology to identify songs being played on various platforms. Revelator maintains a blockchain platform based on Ethereum. The smart contract architecture is designed to enable accurate real-time splits of rights holders' royalty positions, providing enhanced visibility for clearance and settlement of royalty transactions. Payments are automatically distributed to all the stakeholders at the same time.[33] Revelator sends queries to BMAT every two hours. When BMAT returns "play data" for one of the compositions involved in the prototype, Revelator deposits a transaction on its Original Works platform through a smart contract that determines which rights holders get paid and how much. Payments are made in Original Works tokens. The rights holders will be able to convert those tokens to the paper currency of their choice once the project reaches that stage. This system enables near-real-time payments for public performances of musical works instead of the conventional scheme of payments, for example 45 days after the end of each quarter.[34]

5. Enforcement of IP rights and fight against counterfeits

A case decided in June 2018 in the Peoples Republic of China clearly shows that blockchain technology can play an important role in dealing with infringements of intellectual property rights. There, the Hangzhou Internet Court had to decide whether information from a rights holder

[32] Now that European collecting societies are allowed to compete across borders, smaller societies like Teosto need to be innovative to compete with their larger counterparts such as SACEM in France and GEMA in Germany.

[33] Available at: https://www.prnewswire.com/il/news-releases/revelator-launches-the-first-digital-wallet-app-for-artists-and-music-makers-moves-entertainment-industry-toward-instant-royalty-payments-300855100.html (accessed: 24 Feb 2021)

[34] The streaming platform Choon, which provides "service[s] for independent musicians and [a] digital payments ecosystem powered by the Ethereum blockchain". Available at: https://datatransmission.co/news/blockchain-streaming-platform-choon-announces-next-phase/ (accessed: 24 Feb 2021), launched in mid-2017. However, as of late 2019 and due to a "significant downturn in the crypto market", Choon announced a partnership with Emanate, another platform which enables realtime payments and digital contract automation for the music industry based on distributed ledger technology. Available at: https://emanate.live/home (accessed: 24 Feb 2021]

stored in a blockchain about actual violations could be credible evidence.[35] The Court ultimately affirmed this to be the case.

The case was about unauthorized public access to copyrighted content. The rights holder (and plaintiff) had made screenshots of the websites with the disputed publications and had them saved by an external service provider, the evidence preservation platform Baoquan.com. Baoquan uses the Bitcoin blockchain for storage and the blockchain-based document security platform Factom. Baoquan captures images from a target webpage by automatically employing Puppeteer (an open source program by Google) and at the same time acquires the source code of the target webpage by employing curl. To save space, only the hash of the relevant data is saved.[36] This hash can, however, be only reproduced by the person who owns the unchanged original file with the aid of an encryption program.

In the decision, the court dealt extensively with the evidential value of the information stored in this way, e.g. the webpage screenshots captured through Puppeteer that demonstrated the alleged infringing article published by the defendant in 2017 was substantially consistent with the article at issue. It recognized the value as particularly high because the evidence preservation platform was an independent third party. The blockchains used were also considered to be particularly secure due to the number of network nodes involved. The Court stated in particular: "This evidence securing system is equally open to all people and anyone can use the system. Moreover, the operation process thereof is automatically completed by a machine, according to a program preset by the evidence obtaining system. The likelihood that relevant links are tampered with by humans throughout the evidence obtaining and evidence securing process is relatively low. Therefore, the source of the electronic data has relatively high credibility; […]. In the absence of evidence to the contrary, therefore, this court confirms that the approach by Baoquan.com to parse a domain name for a target webpage to generate and store digital messages by using public open source capture programs from Google is reliable."[37]

This example shows the important role distributed ledger technology already plays in proving infringements of intellectual property rights — and the role it can still play in the future. This is because it is often difficult

[35] Judgement of June 27, 2018-055078. No. 81. Available at: https://go.dennemeyer.com/hubfs/blog/pdf/Blockchain%2020180726/20180726_BlogPost_Chinese%20Court%20is%20first%20to%20accept%20Blockchain_Judgment_EN_Translation.pdf. (accessed: 24 Feb 2021)

[36] Ibid.

[37] Ibid.

to actually prove that an intellectual property right has been violated or — at least — to what extent an infringement has occurred.

6. Summary and outlook

This article points out the importance and potential areas of application of distributed ledger (blockchain) technology in general and smart contracts in particular with regard to intellectual property rights — today and possibly in the future. There is no denying that the new technology poses technical and legal challenges. However, such concerns do not fundamentally speak against the future use of distributed ledger technology in the area of intellectual property.

First, it was shown that the described possibility of seamless and tamper-proof storage of information about the process of invention in the blockchain could be used to document the "state of the art". This is necessary for technical inventions in order to prove the patentability of an invention. Using such information, it would also be possible, however, for patents to be challenged if the protected technology was not new and/or did not go beyond the known state of the art. The related proof of priority could also play a similarly key role with other intellectual property rights, such as design rights and trademarks.

Given the special challenges of co-inventions and in the context of R&D cooperations, through information stored on a blockchain it could also be proven who (and to what extent) contributed to an innovation process, which is helpful for the specific assignment of the result. In the case of works protected by copyright, the creative process could be documented in a comparable way, here in particular to prove the authorship. Overall, the blockchain would thus function as a reliable digital register.

Technical and non-technical information not protected by exclusive rights are of enormous economic importance for companies. However, such information is only really valuable if it is not obvious. The storage of trade secrets in a blockchain could suffice to fulfill the requirement of an effective and, importantly, an appropriate protection of secrets. By using this technology, the strict requirements of the new European law on the protection of trade secrets could be met. The extent to which a blockchain is ultimately able to ensure effective protection of trade secrets (know-how) depends both on the respective technical design and, crucially, on who actually has access to the information concerned.

Another important area of application for blockchain technology and smart contracts lies in the documentation of the transfer of protective rights,

the granting of licenses and the transfer of licenses. Such evidence is particularly important for the holder of a legal position, who has to prove the existence of this legal position — and thus an intact "chain of rights" or licenses — for example in order to be able to counter the accusation of unauthorized multiple use. The licensor may have the ability to check whether an intellectual property right (in particular licensed software) has only been used to the extent permitted by the respective contractual framework (licensing agreement).[38] Given the specific situation of the transfer of "used" software, the assignment of a license to an authorized person could become more readily verifiable.

Last but not least: in the case of infringement of intellectual property rights, a recent decision in China has shown vividly the high evidentiary value that can be attributed to the information stored in a blockchain. It remains to be seen to what extent this will also be the case before German and European courts. However, as the Hangzhou Internet Court stated in the case described above: "Technical means like blockchain should be analyzed and determined case by case with an attitude of being open and neutral. Distributed ledger technologies should not be dismissed nor the burden of proof raised because they are novel and complex."

References

Allessie D. et al. (2019) Blockchain for digital government: An assessment of pioneering implementations in public services. In: Pignatelli F. (ed.) JRC Science for Policy Report. European Union. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf. (accessed: 24 Feb 2021)

Blocher W., Hoppen A., Hoppen P. (2017) Softwarelizenzen auf der Blockchain. *Computer und Recht*, no 36, pp.337–348.

Chohan U. (2017) The Double Spending Problem and Cryptocurrencies. Available at: https://ssrn.com/abstract=3090174 (accessed: 24 Feb 2021)

Clark B. (2018) Blockchain and IP Law: A Match made in Crypto Heaven? Available at: https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html. (accessed: 24 Feb 2021)

Dob D. (2018) Permissioned vs Permissionless Blockchains: Understanding the Differences. Available at: https://blockonomi.com/permissioned-vs-permissionless-blockchains/ (accessed: 24 Feb 2021)

[38] In relation to copyright, blockchain technology and blockchain-based smart contracts could also play a future role as a tool in Digital Rights Management; see for a general overiew [Finck V., Moscon V., 2019: 79].

Finck M. (2019) *Blockchain Regulation and Governance in Europe.* Cambridge (Mass.): University Press, 255 p.

Finck M., Moscon V. (2019) Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC*, no 1, pp. 77–108.

Fulmer N. (2019) Exploring the Legal Issues of Blockchain Applications. *Akron Law Review*, vol. 52, pp. 161–192.

Gürkaynak G. et al. (2018) Intellectual property law and practice in the blockchain realm. *Computer Law Security Review*, vol. 34, pp. 847–862.

Hauck R. (2017) Der Erschöpfungsgrundsatz im Patent- und Urheberrecht, EuZW, vol. 28, pp. 645–649.

Hilty R. (2018) Kontrolle der digitalen Werknutzung zwischen Vertrag und Erschöpfung´. *GRUR*, vol.120, pp. 865–880.

Hohn-Hein N., Barth G. (2018) Immaterialgüterrechte in der Welt von Blockchain und Smart Contract. *GRUR*, vol. 120, pp. 1089–1096.

Hoppen A., Hoppen P. (2018) License on Blockchain: Transferring and Managing Software Licenses on the Ethereum Blockchain, Version 1. Available at: https://github.com/license-on-blockchain/whitepaper/releases (accessed: 24 Feb 2021)

Kaulartz M., Heckmann J. (2016) Smart Contracts — Anwendungen der Blockchain-Technologie. *Computer und Recht*, no 35, pp. 618–624.

Kraßer R., Ann C. (2016) *Lehrbuch Patentrecht*. 7th ed. Munich: Beck,

Kuchta R. (2017) The hash — a computer file's digital fingerprint. Available at: https://newtech.law/en/the-hash-a-computer-files-digital-fingerprint/(accessed: 24 Feb 2021)

Lauber-Rönsberg A., Hetmank S. (2019) The Concept of Authorship and Inventorship under Pressure: Does Artificial Intelligence Shift Paradigms? *GRUR International* no 4, pp. 641–647.

McJohn S., McJohn I. (2016) The Commercial Law of Bitcoin and Blockchain Transactions. Legal Studies Research Paper no 16–13. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874463(accessed: 24 Feb 2021)

Nakamoto S. (2008) Bitcoin: A Peer-to-Peer Electronic CashSystem. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 24 Feb 2021)

O'Shields R. *(2017) Smart Contracts: Legal Agreements for the Blockchain. N.C. Banking Institute,* no 21, pp. 177–194.

Pahlow L. (2017) Patentlizenz und Patentlizenzvertrag. In: Henn/Pahlow (eds.) Patentvertragsrecht. 6th ed. Heidelberg: C.F. Müller, 401 p.

Pilkington M. (2016) Blockchain Technology: Principles and Applications. In: Olleros F., Zhegu M. (eds.) Research Handbook on Digital Transformations. Cheltenam: Elgar, pp. 225–253.

Raskin M. (2017) The Law of Smart Contracts. *Georgetown Law Technology Review,* no 2, pp. 305–341.

Reinbothe J. (2015) Collective Rights Management in Germany. In: Gervais D. (ed.) Collective Management of Copyright and Related Rights. 3rd ed. The Hague: Kluwer Law International, pp. 215–250.

Rosenblatt B. (2019) Blockchain Applications for Music Enter the Bowling Alley. Available at: https://copyrightandtechnology.com/2019/06/15/blockchain-applications-for-music-enter-the-bowling-alley/ (accessed: 24 Feb 2021)

Ross E. (2017) Nobody Puts Blockchain In A Corner: The Disruptive Role of Blockchain Technology. *Catholic University Journal of Law and Technology,* vol. 25, pp. 353–386.

Sai Deepak J. (2010) The Elusive Quest for the Definition of Obviousness — Patent Law's Holy Grail. *IIC*, no 4, pp. 410–427.

Salmon J., Myers G. (2017) Blockchain and Associated Legal Issues for Emerging Markets, EM Compass. Available at: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F (accessed: 24 Feb 2021)

Schrey J., Thalhofer T. (2017) Rechtliche Aspekte der Blockchain. *NJW,* vol. 70, pp. 1431–1436.

Sergey I. (2018) Scilla: a Smart Contract Intermediate-Level Language. Available at: https://arxiv.org/pdf/1801.00687.pdf (accessed: 24 Feb 2021)

Szabo N. (1997) The Idea of smart contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (accessed: 24 Feb 2021)

Tapscott D., Tapscott A. (2016) *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* N.Y.: Random House,

Walch A. (2017) The Path of the Blockchain Lexicon (and the Law). *Review of Bank and Fin Law,* vol. 36, pp. 713–765.

Yanisky-Ravid S., Kim E. (2019) Patenting Blockchain: Mitigating the Patent Infringement War. Available at: C:/Users/Juristische%20Fakultät/Downloads/SSRN-id3357350.pdf. (accessed: 24 Feb 2021)

Zurth P. (2020) Lizenzverträge und Lizenzen in der Insolvenz und Einzelzwangsvollstreckung. In: Obergfell E., Hauck R. (eds.) Lizenzvertragsrecht. 2nd ed. Berlin: De Guyter, pp. 183–225.

Rights to Intellectual Works Generated with Artificial Intelligence: A Russian View in the Global Context

Vitaly Kalyatin

Associate Professor, Department of Theory of Law and Interdisciplinary Studies, National Research University Higher School of Economics, Doctor of Juridical Sciences. Address: 20 Myasnitskaya Str., Moscow 101000, Russia. E-mail: kalvit@yandex.ru

Abstract

The broad use of artificial intelligence in creating intellectual works poses difficulties for legislators and courts in choosing the proper legal framework for such works and defining the place of artificial intelligence in the legal system as a whole. In this article, we shall study different models of regulating such issues and analyze the prospects and consequences of their use. We show that only a few of many different models for copyrighting AI-generated works are viable and that the most promising among them is the introduction of a special limited related right for the person who organizes the use of the AI application. This model resembles already existing civil law approaches to protecting the rights of phonogram producers, broadcasting and cablecasting organizations, and database creators. Thus, the inclusion of artificial intelligence into the IP domain does not require reconstructing the legal framework but only adapting existing approaches.

Keywords

intellectual property, artificial intelligence, authors' rights, related rights, author, creative activity, creativity, public domain, user, investor, organizer of AI use.

For citation: Kalyatin V.O. (2021) Rights to Intellectual Works Generated with Artificial Intelligence: A Russian View in the Global Context. *Legal Issues in the Digital Age,* no 1, pp. 42–63.

DOI: 10.17323/2713-2749.2021.1.42.63

Introduction

The protection of AI-generated intellectual works is a topical legal issue today: the growing possibilities of modern computers, on the one hand, and their broad involvement in the process of creating intellectual works,

on the other, pose the question of choosing the right legal framework for works generated by artificial intelligence. The diversity of potential approaches to regulating relations in this domain requires the selection of basic models, which would then be developed to cover all possible cases. Such systematization would allow choosing fundamental approaches to solving the posed problem and adapting them to specific countries.

Nevertheless, the problem of determining the copyright owner of such works is much more important than solving the purely practical task of protecting the resulting rights. Already today, AI-generated outputs are often virtually indistinguishable from human-made works or even surpass the latter in popular opinion.[1]

Mankind must therefore take a stance (in particular, in the legal domain) on intellectual property not created by man, which is becoming increasingly common today.[2] Moreover, the role of electronic technologies in human life will only grow with time, leading to an ever greater number of civil law issues involving AI. The resolution of this seemingly minor problem may have a major impact on the further development of civil law.

1. Definition of artificial intelligence

By its nature, artificial intelligence (AI) may be considered to be computer software, which is a well-developed notion in law. However, the most common approach to AI today is to view it as an instrument used in human activity and thus as an object of law. As a result, the question of rights to an AI-generated work is replaced to all intents and purposes by the question of whether a person made a creative contribution to its generation (the use of creativity in the generation of a work is considered a key aspect today for determining the work's protectability).

On the one hand, this allows the application of traditional approaches to regulating rights to such intellectual works in order to settle copyright issues with the help of law. On the other, it weakens the protection of

[1] During a study conducted by Rutgers University (USA) in 2017, a group of computer scientists and art historians were unable to tell paintings generated by artificial intelligence apart from paintings made by human beings. In a number of cases, paintings generated by AI were given higher assessment. Autonomous "creation": Authorship and protectability // Lauber-Rönsberg: Autonome "Schöpfung" — Urheberschaft und Schutzfähigkeit GRUR 2019, 244. Beck-online.

[2] As, for example, in the controversial case of "monkey selfies" made with the camera of photographer D. Slater. Available at: https://en.wikipedia.org/wiki/Monkey_selfie_copyright_dispute (accessed: 16.04.2020)

works whose generation did not involve a creative contribution by a human being.

The situation is somewhat simpler in common law jurisdictions, where a softer criterion of creativity is used. Nevertheless, this does not eliminate the risks to human creativity that arise from the mass use of computer systems.

This scenario is a lot more difficult to implement in civil law jurisdictions, including Russia.

Thus, it is not sufficient simply to weaken the criteria for the protected object; one must also introduce regulations that take the specific nature of AI use into account.

Computer systems can be used to different extents to generate intellectual works: the degree of their participation can range from the simple fixation of an object (text, photograph, sounds) to the complex processing of material in which the role of the user of the computer system simply involves selecting the task or initial material.

Clearly, when the computer system is only used as an instrument for recording the user's activities, no major regulatory problems arise. The same holds when a user processes material (e.g., a photograph or text) with the help of a computer that acts as a technical device for changing or checking the material in accordance with the user's instructions.

The problem arises when the computer acts without any direct human participation in the process. Although a person may, in fact, play a role in the process by, say, formulating the principles of action or rules of behavior of the computer system, the latter acts as an autonomous system during the actual problem-solving process (even if a certain degree of user participation in the situation is required).

In view of the above, we may take as a basic definition the version proposed by the World Intellectual Property Organization: "Artificial intelligence (AI) is a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention." In the narrow sense, this term refers to "techniques and applications programmed to perform individual tasks."[3]

[3] WIPO conversation on intellectual property (IP) and artificial intelligence (AI), 2nd session. 2020. Available at: https://www.wipo.int/meetings/en/details.jsp?meeting_id=55309 (accessed: 25.11.2020)

Although such a definition is fairly convenient for limiting the field of study, one must keep in mind that assessing the necessity for the participation of human intelligence in solving a problem remains extremely subjective.

When considering these issues, one must note that AI is no analogue of human intelligence either in its organization or in its operation. In this regard, it is useful to recall John Searle's thought experiment called "the Chinese room argument" [Searle J., 1990: 26–31]. It goes as follows: if a person shut up in a room is given instructions about how and when to use Chinese hieroglyphs to respond to a question in Chinese, he will be able to answer questions, and his responses may appear intentional and reasonable to a Chinese speaker outside the room. Nevertheless, the person shut in the room does not, in reality, understand the meaning of the questions or his answers.

This thought experiment shows the theoretical possibility of organizing information processing in such a way as to generate well-founded and seemingly reasonable answers through the mechanical use of preset rules of action and examples of analogous tasks ("weak AI"). The application of weak AI is naturally limited to the range of tasks for which it is programmed; in contrast, "strong AI" should be able to solve problems in virtually any field. However, no systems developed so far permit us to speak of the existence of strong AI.

At the same time, neural networks are capable of self-learning, which can be potentially used to create strong AI.

Law and legal doctrine also employ other definitions of AI. For example, GOST standard #15971-90 (Table 1, item 56) defines AI as the "capacity of a computer to model the thought process by performing functions that are usually associated with human intelligence. Examples of such functions include learning and logical reasoning."[4] In turn, item 5 of the Russian National Strategy for the Development of Artificial Intelligence up to the Year 2030 defines AI as "the set of technological solutions used for imitating the cognitive functions of man (including self-learning and searching for solutions without any preset algorithm) and for obtaining results in implementing specific tasks that are at least comparable with the results of human intellectual activity. This complex of technological solutions includes ICT infrastructure, software (including software employ-

[4] GOST 15971-90. State standard of the USSR. Information processing systems. Terms and definitions (approved and enacted by the Decree of the Committee for Standardization of the USSR no 2698).

ing machine-learning methods), and processes and services for processing data and finding solutions."[5]

While many other definitions of AI exist in different countries, they generally either draw analogies with human intellectual activity or list specific functions performed by artificial intelligence.

An example of the first type of definition is the Singapore National AI Strategy that characterizes AI as the capacity to model human intellectual activity with the help of a computer.[6] In turn, the UAE National Program for Artificial Intelligence defines it as the set of technologies that allow a machine or system to understand, learn, act and feel as a human being. Such approaches are quite understandable: they make it possible to regulate this domain without getting bogged down in theoretical discussions. Nevertheless, they are not very productive, as there is an enormous difference between the organization of human intelligence and the operation of electronic devices. As a result, all attempts to compare them shall always remain tentative and superficial.

Definitions of the second type are currently being discussed in the EU and USA. For example, the European Resolution proposes the following criteria of "smart autonomous robots": (1) acquisition of autonomy through sensors and/or by exchanging data with the environment and trading and analyzing such data, (2) self-learning from experience and by interaction, (3) at least a minor physical support, (4) the adaptation of behavior and actions to the environment, and (5) the absence of life in the biological sense.[7] The Future of Artificial Intelligence Act currently under discussion in the USA defines AI as any artificial systems that (1) perform tasks under varying and unpredictable circumstances, without significant human oversight, or learn from their experience and improve their performance, or (2) think like humans, or (3) act like humans (such as systems that can pass the Turing test or other comparable tests), or (4) seek to approximate some cognitive task, or (5) act rationally and achieve goals via

[5] Russian Presidential order no 490 "On the development of artificial intelligence in the Russian Federation" (together with the National AI Development Strategy until 2030) // SPS Consultant Plus.

[6] Available at: https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_%D1%81.%204, 12 (accessed: 25.11.2020)

[7] European Parliament resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). 2017, February 16. Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN (accessed: 16.04.2020)

perception, planning, reasoning, learning, communicating, decision making, and acting.[8]

Similar criteria have been proposed by Russian specialists. For example, V. Naumov and E. Tytyuk have formulated the following characteristics of an AI application: (1) created for processing information, (2) able to analyze information about the environment, (3) autonomous implementation of algorithms, and (4) capacity for self-learning during implementation without human interference [Naumov V.B., Tytyuk E.V., 2018: 533].

All the aforementioned criteria mostly pertain to the decision-making process of AI rather than its intrinsic nature. At the same time, the conformity of a computer system to these criteria says nothing about the quality of the results. Clearly, when assessing the protectability of an intellectual work, the user cannot take the organization of the computer system into account. For the purposes of protecting IP, one should therefore treat AI as a "black box" and only assess the intellectual work itself.

To this end, it is important to define the criteria that such an intellectual work must conform to.

2. General approaches to copyrighting AI-generated intellectual works

In its Plenary Decision no 10 "On applying § 4 of the Civil Code of the Russian Federation" of April 23, 2019, the Russian Supreme Court wrote, "When examining cases of attributing authors' rights to a specific intellectual work, courts should keep in mind that, by the import of §§ 1228, 1257 and 1259 of the Civil Code of the Russian Federation taken together, only intellectual works resulting from creative activity are subject to such rights. One should also keep in mind that, until established otherwise, an intellectual work must be the result of creative activities. It should be also kept in mind that the lack of novelty, uniqueness and/or originality *per se* in an intellectual work does not necessarily indicate that such a work is not the result of creative activity and thus is not subject to authors' rights. The creative nature of a work does not depend on whether the work was made by an author on his own or with the help of technical means. At the same time, works made with technical means without any human creative activity (for example, photos and videos made by an automatic video camera used for recording civil infractions) are not subject to authors' rights" (item 80).

[8] H.R. 4625. Future of artificial intelligence act of 2017, 115th Congress (2017–2018). Available at: https://www.congress.gov/bill/115th-congress/house-bill/4625/text (accessed: 19.06.2019)

Thus, with regard to the protectability of intellectual works, current Russian judicial practice makes a distinction between a work made by a human being and a work made by a machine without human participation. Such an approach is used in other countries, too. For example, the US Copyright Office registers intellectual works only if they are created by human beings,[9] while courts systematically reject all attempts to attribute copyrights to works not made by humans (e.g., works made by an animal[10] or by the holy spirit[11]). Some countries qualify this by insisting on the creative nature of the activity used to make the work,[12] while others explicitly specify that an author can only be a human being.[13]

The stress on the creative nature of a work makes it impossible (within the framework of the current Russian model) to protect AI-generated works. This may require changing the current criteria of the protectability of such works. Such an approach is based on the importance attached to creativity today.

Thus, if we want to extend authors' rights to AI-generated works, we must either change our approach to the criterion of creativity (for example, by interpreting this criterion more broadly so as to extend it to AI-generated works or take different approaches to copyrighting human-made and AI-generated works.

We should note in this regard that the selection of criteria for the protectability of works cannot be considered separately from the designation of the person in whom the author's right is vested. Irrespective of the approach, the choice of criteria and the rights holder is determined by the social goals of copyrighting.

These goals lie in several different planes.

The main goal of copyrighting IP is to stimulate socially significant work for creating such property. This is shown by the choice of both the rights holder and the conditions of protecting the property. The introduction of copyrighting has encouraged authors to create new works, as the

[9] Compendium of U.S. Copyright Office practices. Para 306. 2017. Available at: https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf (accessed: 20.06.2019)

[10] Naruto v. Slater, #16-15469 (9th Cir. 2018).

[11] U.S. Court of Appeal Ninth Circuit June 10, 1997, Urantia Foundation v. Maaherra, 114 F.3d 955, 963–964.

[12] For example, §2 of the Copyright law of Japan stipulates that only works that creatively express thoughts or emotions are copyrightable.

[13] Cf., for example, §7 of the German act on copyright and related rights.

main incentive of human behavior, at least in today's paradigm, is to improve one's material status [Karapetov A. G., 2016: 46]. In this regard, the stress on creativity leads to an increase in the stimulating effect thanks to moral factors (recognition of a person as an author). Indeed, moral incentives are often the most significant for authors, as they lead to the societal recognition of a person's uniqueness, special traits (talent), etc.

Nevertheless, it is important to keep in mind that copyrighting aims not only to recompense authors out of gratitude or fairness but also (and more importantly) to stimulate socially significant activities on their part.

At the same time, copyrighting IP stimulates not only the creation but also the disclosure of such works. To allow a person to derive profit from reproducible IP, a monopoly must be awarded to him. If the legislator does not create a legal monopoly (exclusive right), the author is obliged to maintain a factual monopoly — in particular, by keeping his intellectual work a secret. Nevertheless, such a state of things does not correspond to the goals of IP law [Sesitsky E. P., 2018: 133].

From the economic standpoint, assigning a right to a specific person is necessary to assure economic turnover, as the very development of a right is possible only on the condition of the clear-cut identification of the original rights holder. As Professor Dozortsev once said, "The creative result of intellectual activity bears the imprint of the author's personality. Thus, the original proprietary right of use, based on creative activity, is tied to the person of the author. And it is less a matter of protecting the interests of a person as such than of assuring normal economic turnover. Thus, authorship is important first and foremost as grounds for the emergence property rights and as the original point of reference for these rights: it is the result of the individualization of the original rights holder" [Dozortsev V.A., 2003: 145].

This goal is even more important in common law jurisdictions: "By recognizing and exploiting the fact that the law supported the view that an author was creating a piece of property which could be assigned a financial value, it became possible to move away from private to commercial patronage" [Feather J., 2010: 364]. This stimulates the consumption and commercial use of intellectual works and thus their creation.

Regardless of the jurisdiction to which a country belongs, both goals play an important role, even if legislators have different priorities. As one paper states, "…it is true to say that in the development of modern copyright laws, the economic and social arguments are given more weight in the Anglo-American laws, whereas, in Continental law countries, the natural law argument and the protection of the author are given first place" [Garnett K., James J., Davies G., 1999: 29].

Another goal is to allocate responsibilities during the circulation of rights. Nevertheless, this consideration does not play a major role, even if it should be kept in mind, as we will see when we discuss the model of attributing rights for a generated work to AI itself.

Finally, regulations in this domain can also try to lower the concomitant risks. Although AI is very important in contemporary society, its use also harbors certain dangers. AI is potentially capable of producing major problems for individuals engaged in intellectual activities, as human authors shall never be able to compete with AI in the speed and cost of creating new intellectual works in areas of mass production (especially in domains without high standards for the artistic value of the created works). If AI-generated works are not protected, they will be used to an ever greater extent by society to the detriment of human authors.

The aforementioned danger can be lowered by the timely introduction of a system for protecting AI-generated intellectual works involving greater limitations than usual authors' rights for similar intellectual works — in particular, in the duration and, possibly, extent of rights and cases of free usage. Although such a danger is still hypothetical today, its most effective solution involving the introduction of a limited right is possible when no commonly accepted approach has yet emerged in legislation or court practice (such as the recognition of full-fledged authors' rights for such objects).

In the final account, it is the legislators' goals that determine the choice of works whose creation shall be stimulated through the selection of rights holders and copyright criteria.

Numerous criteria of protectability are used in the world for works of authorship: novelty, uniqueness, originality, individuality, etc. Despite their diversity, they generally aim to stimulate the creation of intellectual works, on the one hand, and to limit the range of these works, on the other. For this reason, it would be insufficient to consider the "novelty" of works. Whereas it is possible to verify the novelty of a created work in the case of patent law, this is much more difficult to do in practice for works of authorship.

An even more important consideration is that the benefits from the introduction of an exclusive right (of a monopolistic nature) outweighs the negative consequences for society only in the case of socially significant intellectual works that cannot be created by everyone.

Thus, the criterion of creativity is aimed at defining the qualitative characteristics of a work that make it stand out among all works made by hu-

man beings. Today, we can assess the nature of human intellectual activity only through its results. Thus, when we speak about the creativity of the author, we actually mean its reflection in the finished work, which serves as a reflection of human activity.

Nevertheless, it is not easy to make such assessments of a created work. As a result, courts tend to take other criteria into account, too. In particular, the Russian Supreme Court noted in 2006 that works of authorship include works that can be used independently and that are creative and original;[14] the Court for Intellectual Property Rights used the criterion of uniqueness;[15] one court of arbitration employed the criteria of originality and novelty;[16] and so on.

In actual fact, the aforementioned criteria have no independent significance; rather, they are special cases of the criterion of creativity. For this reason, they can be used to facilitate the assessment of a work yet not to replace the criterion of creativity. This is why the Russian Supreme Court in its plenary decision cited above ruled that the lack of novelty, uniqueness and/or originality of a work of authorship does not in itself show that the work is not creative and thus that it is not copyrightable.

The criterion of creativity is used in continental law jurisdictions as well as in some common law countries (USA, Singapore). However, orientation on human inner psychological processes makes it difficult to use this criterion for assessing AI-generated intellectual works. Even if the rights holder is taken to be a person (programmer, user, etc.), the problem will still remain: it will not be easy to show that the work is creative or even that making such a work necessarily requires creativity.

Still, it is extremely important to continue to make qualitative assessments of intellectual works, as the use of electronic systems can lead to a multifold increase in the number of intellectual works without any utility for society.

At the same time, one can attain the same goals without the complicated process of assessing the intellectual activity of a work's creator. An example is the use of "qualitative" criteria in patent law: the criterion of inventiveness and analogous criteria such as the "inventive step," significant novelty, etc.

---

[14] Section 21 of the Plenary decision of the Supreme Court of the Russian Federation no 15 "On handling civil cases relating to the application of law on authors' and related rights." 2006, June 19. (Expired) // SPS Consultant Plus.

[15] Decision of the Court for Intellectual Property Rights on case no A12-18806/2013.

[16] Decision of the Court of Arbitration of the Sverdlovsk Oblast no A60-49303/2015.

We thus see that, in the different models for copyrighting AI-generated intellectual works, the criteria for the protectability of such works should take the differences between AI operation and human intellectual activity into account.

3. Models of protecting AI-generated intellectual works

Theoretically, the following persons participating in the creation of intellectual works could be vested with copyrights in these works:

the person who develops the program on which the AI application is based;

the person who organizes the operation of the AI application that generates the intellectual work (for example, the investor in the project);

the user of the AI application;

the AI application itself;

Intermediate models are also possible: co-authorship between AI and a human being and fictional authorship.

One should also consider the possibilities of putting AI-generated works subject in the public domain and of excluding such works from copyright altogether.

None of these approaches has received unanimous support so far. Moreover, as one specialist has noted, all these concepts "have both advantages and disadvantages. None of them is fully adequate or fully wrong, and the full-fledged implementation of any of them will require a minor or major reform of existing law, including IP law" [Morkhat P., 2019: 240–241].

A) The person who develops the AI application

This approach may seem fairly straightforward, as it calls for applying already existing copyright criteria to intellectual works. In this case, AI is simply treated as an instrument that the author uses to create new intellectual works — a model that is well known in law.

Such an approach is set forth, for example, in a bill for amending §1228 of the Russian Civil Code that was introduced to the State Duma by deputy A. Kobilev.[17]

[17] Shestoperov D. Chto napisano softom. Plody iskusstvennogo intellekta zapishut za razrabotchikami [What is written by software: Rights to results of artificial intelligence

At the same time, it is important to note that the author of the AI application largely predetermines its operation yet makes no contribution to the resulting work. For this reason, he cannot be viewed as the author of the works generated by the AI application, which would lead to a totally new approach in which the author's rights would extend to a group of intellectual works that the author did not create, as he only prepared the instrument for the user.

Such a situation would mean stimulating the creation of AI applications rather than the creation of intellectual works, i.e., the author would be stimulated to create new versions of AI applications (that may subsequently create an even greater number of new intellectual works) yet not to create new works of higher quality, as he does not participate in the process of applying these AI applications.

This would have a negative impact on society in general and on persons using AI in particular, as the latter would not receive any rights to the works created by their companies. In reality, software buyers usually expect to hold rights in the products they create with this software, and the existing concept of authors' rights agrees with this view.

At the same time, the approach discussed here would inevitably lead to market monopolies, as the rights to an enormous number of generated works shall be accorded to a few leading AI developers rather than to the multitude of competing persons using AI in their work.

Moreover, AI developers already receive sufficient compensation from selling rights to their products.

B) The person who organizes the operation of the AI application and its generation of intellectual works

A different situation arises when one focuses on the person who organizes the AI application's generation of intellectual works. Such a person may have access to the corresponding software in different ways: as the owner of an exclusive right or as a license holder or simply as the owner of the hardware on which the software is installed — this makes little difference.

Grounds for granting rights to such a person may include the recognition of the public utility of his activities and the need to encourage them. In particu-

shall be accorded to developers]. Available at: https://www.kommersant.ru/doc/4566144?query=%D0%9A%D0%BE%D0%B1%D0%B8%D0%BB%D0%B5%D0%B2 (accessed: 10.11.2020)

lar, during the discussion of AIPPI results, French jurists voiced the opinion that, with regard to copyrighting AI-generated works, the rights to the works should be granted to persons that initiated the creation of the works, managed the projects, and disclosed the works (by analogy with collective works mentioned in § L.113-5 of the French Intellectual Property Code).[18]

A similar theory was advanced by the German scholar Kummer, who argued that a person should be entitled to rights to a work for simply finding and disclosing it ("presentation theory") [Kreutzer T., 72, 73].

Nevertheless, the attempt to recognize such a person as the author does not fully correspond to the principle of authors' rights, and it is not surprising that this theory is fairly actively criticized in Germany today. It would be a lot more logical to speak not of an author's right but of a narrower related right and of a right granted to the organizer of the process of the work's creation, similar to the rights of phonogram producers, broadcasting and cablecasting organizations, etc. Related rights are the area where most German specialists try to place the rights to the objects discussed here [Selvadurai N., Matulionyte R., 2020: 536].[19]

The advantage of this model is the fact that it stimulates the process of the creation of new intellectual works and gives the owner of an AI application the possibility of commercially exploiting it. At the same time, this model may attribute rights to the created works directly to the organizer of the process rather than to the natural person who uses the AI. This would deprive the natural person of any incentives to engage in creative activities. However, in view of the growing possibilities of AI, the user only performs technical functions in most cases, and his activities are rarely creative. This situation is basically similar to cases in which the law gives direct rights to organizers of certain activities such as making databases or phonographs and not to the operators that input the data into the system.

This model is already being implemented in some countries, including the United Kingdom (where it is set down by law) and the USA (court practice). It is also recognized by some other countries such as New Zealand [Selvadurai N., Matulionyte R., 2020: 543].

In Great Britain, the Copyright, Designs and Patents Act stipulates that computer-generated works can be copyrighted even in the absence of a hu-

[18] Study question AIPPI 2019: Copyright in artificially generated works. Para 7. Available at: https://aippi.soutron.net/Portal/DownloadImageFile.ashx?objectId=5292 (accessed: 15.01.2020)

[19] Ibid. Para 13, 18.

man author:[20] a work is considered to be made by the person who makes the necessary preparations for its creation.[21]

There exist different interpretations of this law. For example, D. Vaver asserts that it creates the figure of a "fictional author" on grounds that have nothing to do with stimulating human creativity but only with protecting the object of investments from unscrupulous practice and misappropriation [Vaver, D., 1994: 162]. Other specialists say that the law is sufficiently broad to cover both the person who operates the computer and the person who provides or programs the computer [Bently L., Sherman B., 2004: 117]. Nevertheless, it should be said that it does not cover persons who perform purely technical functions (e.g., users inputting data into the device's memory) and thus once again privileges the organizer of the process.

Without a doubt, the role of the organizer of the process of generating an intellectual work is becoming increasingly decisive and, from the standpoint of public progress, merits to be rewarded. However, this model can be fully implemented only if special regulations are added to the law — for example, in the category of related rights. This will also make it possible, through the introduction of different frameworks, to demarcate human activity from AI operation and thus to minimize the risk of "deflating" the value of intellectual works as a result of the mass production of AI-generated works.

Yet would it not be better to stress investments rather than organizational activities and vest rights in persons investing in the development of an intellectual work? Such a model is implemented in the case of, say, database creators. Consequentially, it has been proposed to give priority to the investor in the case of intellectual works, too.[22]

Nevertheless, it should be said that the law connects the notion of the database creator first and foremost with organizational efforts (for example, § 1333, item 1, of the Russian Civil Code stipulates that "The database creator is a person who organizes the creation of the database and the work of collecting, processing and inputting its materials"), whereas the criterion of investments applies to the database itself rather than to the activities of the database creator. In other words, the law focuses on the organizational activity of a person and protects the database creator rather than the investor (e.g., the person who provides funds for the project). This is expressed in a less explicit manner in Directive 96/9/EC of the European

[20] Ibid. Para 9(3), 178.

[21] Ibid.

[22] Study question AIPPI 2019… Para 13, 18.

Parliament and Council of March 11, 1996, on the legal protection of databases; according to § 7, item 1, it is the "database creator" who is protected.

Thus, one should make the notion of the "investor" include organizational functions. This is entirely justified, as organization plays a decisive role in the process of the creation of an intellectual work.

Another question is whether it makes sense to cite the amount of investments in an AI-generated work as an additional criterion of protectability. It seems to us that, with the exception of databases, it would be inexpedient to limit additionally the protection of works of authorship into which major investments have not been made, as AI can be used in highly diverse spheres, some of which do not require any special investments.

C) The user of the AI application

The AI user is a person who directly launches the implementation of the task and determines its parameters. This clearly allows him to pretend to certain rights with respect to the created work.

Moreover, in jurisdictions that do not require any major creative contributions to be made to the work (for example, in the United Kingdom by virtue of the "sweat of the brow" doctrine), any actions on choosing and improving AI-generated works may be considered creative [Samuelson P., 1986: 1185, 1204]. US court practice has precedents of the recognition of "quasi-property rights" (quasi-property treatment) even in the absence of any creative contribution to the work — as in the case of "breaking news" [Yu R., 2017: 1266–1268].

Proposals to give rights to AI users have also been made by Russian specialists [Nazarov N., 2020: 61].

Nevertheless, it must be kept in mind that the role of the AI user can range from exerting a major impact on the generated intellectual work to performing purely mechanical functions by inputting the required parameters into the system. While the activities of the user may be outwardly described in the same terms (such as launching a certain process), the key aspect is the user's awareness of the expected results: only if he has an idea of the characteristics of the future work can his activities be called "creative".

If the AI user's activities have a creative component, he shall be recognized as an author by existing law, too.

Thus, the problem arises when the AI user performs purely technical work. Vesting such a person with rights to created works would not en-

courage him in any way: by the nature of his activities, he only carries out his superior's instructions.

Without a doubt, such rights would stimulate the AI user's employer. The employer would obtain rights from his employees, as the works are created in the framework of employment relations, while getting rights to the works would encourage him to use AI more and to make products of higher quality. Nevertheless, as the original rights are granted to the employees in a random manner due to the technical nature of their activities, the introduction of this added complication seems totally unwarranted. In this regard, the present approach has no advantages over the model described in the previous section.

At the same time, this approach can have a negative impact on the user's activities by stimulating him to search for effective software that would do everything for him instead of trying to create new intellectual works himself [Perri M., Margoni T., 2010: 626]. This is hardly in the interests of society.

D) The AI application

On the whole, legal doctrine has taken a fairly negative view of the idea of vesting rights to intellectual works in the AI application itself.

The crux of the matter does not really lie in the fact that, as some specialists note, computers are unable to protect their own rights or sign contracts on transferring rights to others [Solum L., 1992]. One should note that the absence of human beings is no obstacle to granting rights to a legal entity — an example is the institute of legal persons. Nevertheless, this requires the recognition of the legal capacity and competence of such a person, which needs careful justification. In legal history, the introduction of such entities always results from the necessity to limit the liability of commercial activities, which could also serve as grounds in the present case, as the activities of AI can damage other persons. Indeed, A. Morrigi asserts that the main obstacle to granting rights to AI is the impossibility of making it liable for its actions.

At the same time, the recognition of an entity as being liable requires it to possess certain property — otherwise, it shall be simply used by the owners of an AI application to evade liability. Thus, an AI application would have to be considered liable for its activities and capable of conducting these activities in its own name and making profits from these activities.

Nevertheless, it remains unclear whether the introduction of such a legal entity as AI would give any advantages over the existing institute of the

legal person. Most likely, it would only complicate matters further without producing any positive effects at the present time.

Clearly, AI requires no incentives today, and thus granting it rights would not encourage the development and introduction of new intellectual works.

This explains why this model is not considered seriously by specialists today. However, the situation may change in the future.

E) Co-authorship between AI and human beings

Another way of stimulating a wide group of persons participating in the creation of intellectual works would be to use the institute of co-authorship: for example, viewing the programmer and user as co-authors. Some people have proposed considering the developer of a software program that is capable of self-learning and the user of such a program as co-authors even in the absence of direct cooperation during the creation of the work.[23]

Nevertheless, the advantages of this model are deceptive, as it brings together the shortcomings of the aforementioned models: it stimulates users to borrow others' products, often without making any significant contributions to them [Kumar S., Lavery N.], as well as encouraging the appearance of monopolies of AI developers (by extending their rights to AI-generated products). One should also note that such an approach does not conform to the practice of regulating co-authorship in copyright law, which states that only persons jointly engaged in a creative activity may be called co-authors.

Another model envisages co-authorship between the user (who engages in creative activity, for example) and the AI application. In 1986, the US Congress Office of Technology Assessment criticized an earlier view of computers as passive instruments, noting that the growing complexity of computer programs and the interactive nature of calculations makes it increasingly probable that computers will be recognized as co-authors of human beings in the future.[24]

Nevertheless, such an approach does not provide any evident advantages. Given that the activities of human beings and artificial intelligence

[23] Levy v. Rutley (1871). Available at: https://swarb.co.uk/levy-v-rutley-ccp-1871/ (accessed: 21.12.2019); Hodgens v. Beckingham (2003). Available at: https://www.casemine.com/judgement/uk/5a8ff7a460d03e7f57eb0ad1 (accessed: 10.06.2017)

[24] US Congress, Office of Technology Assessment (1986). Intellectual property rights in an age of electronics and information, 72.

cannot be evaluated on the basis of the same criteria (among other reasons, on account of their totally different organization), relating human and AI rights can make legal approaches a lot more complicated, while AI itself has no need of incentives (at least today).

F) Fictional authorship

Given that most countries copyright only works with authors, one way to solve the problem within the framework of the existing legislation would be to choose a provisional author. For example, in British law the organizer of the creation of a work is factually recognized as the author; a similar approach exists in New Zealand; etc.

Another version of this model is a conception developed by T. Butler [Butler T., 1982: 744–745] that calls courts to select the person who made the greatest contribution to the creation of a work as its fictional author.

It should be said, however, that this model does not define conceptually who should be designated as the fictional author and therefore only offers the advantage of preserving the familiar approach that assumes that every intellectual work has an author. It may therefore be easier to introduce an independent protection mechanism within the framework of related rights without any reference to author status.

G) Public domain/exclusion from copyright

Grounds for not copyrighting AI-generated intellectual works include the lack of creativity (in the current sense) of artificial intelligence. As a result, Russia and many other countries only copyright intellectual works made by human beings, as we noted above. As artificial intelligence does not require any incentives to operate, it is commonly held that one can immediately permit the free use of AI-generated works.

Another version of this approach is to put AI-generated works into the public domain. For example, the United States Copyright Office had stated that works of authorship not created by human beings are in the public domain, i.e., not copyrightable.[25]

It should be said that a work in the public domain is not fully excluded from legal regulation. On the contrary, public domain requires the respect

[25] Compendium of U.S. Copyright Office practice. Para 313.2. Available at: https://copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf, § 313.2 (accessed: 16.10.2020)

of certain rules by persons using the work (for example, indicating the author's name, not making changes to the work, etc.). While the public domain is usually employed for intellectual works whose exclusive rights have expired, there is nothing that prevents it from being used for works that have never been copyrighted at all (see § 1337, item 1, of the Russian Civil Code, §313.6(D) of the Compendium of the United States Copyright Office[26].

The reason to put an intellectual work in the public domain rather than leaving it totally unprotected is to preserve limited public control over its use. However, in the case of AI-generated works, one must define the conditions of their use in law: after all, it is necessary to protect the interests of persons involved in the creation of these objects and the authors of works used in the process.

Still, the main problem of this model is the fact that it eliminates incentives for the development of new intellectual works by AI users. On the one hand, it prevents the AI application's owner from drawing full economic advantages from the created works; on the other, it incites him to conceal his use of AI and attribute the work to a fictional author instead. A recent survey of AI experts showed that over 65% of them believe that computer programs, including AI programs, make the main contribution to creating contemporary works (music, movies, software, etc.).

It is very important to note that the broad application of artificial intelligence runs the risk of excluding human beings from creative activities and establishing new (and real) monopolies on the IP market by AI developers and users. The transfer of AI-generated works into the public domain would only aggravate this problem rather than solving it, as operators of artificial intelligence would begin to conceal its use in their works, attributing them to natural persons who only make a formal contribution to their creation.

One should also take into account the economic implications of public domain. In this regard, it is interesting to consider a model developed by Prof. Arti Kaur Rai of the University of San Diego School of Law. He identifies four categories of societal costs related to the creation and development of IP: (1) labor and capital expenditures on the development of the work, excluding expenditures on transferring rights ("pure development costs"), (2) expenditures on transferring rights ("transaction costs"), (3) costs resulting from lowered incentives for engaging in the corresponding creative

[26] Available at: https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf (accessed: 11.04.2020)

activities resulting from the control of basic research by one copyright holder ("creativity costs"), and (4) expenditures on formulating research that leads to the creation of the work ("invention costs").. Depending on the relation of these four types of costs, one can determine the expediency of putting a given work in the public domain. For example, Rai supports the approach taken by some US universities to encourage the privatization of an intellectual work if the transaction and creativity costs are low and discourage its privatization if these costs are high [Rai A., 1999: 136, 145]. Here, the "pure development costs" and "invention costs" should be measured as the amounts needed to reimburse the corresponding expenditures.

For example, a university that makes a revolutionary discovery in medicine has, as a rule, high invention and transaction costs (to compensate for expenditures on the development of the discovery) as well as high creativity costs (the patent can prevent the development of a whole field of science). For this reason, it would be quite expedient for society to put such a discovery in the public domain.

Let us try to apply this approach to AI-generated intellectual works. The pure development costs are average during the first stage of AI application and fall rapidly thereafter, because artificial intelligence is able to produce a large number of results over a short period of time. The transaction costs are small: a single work can be licensed to a series of users with fairly low expenditures. While the creativity costs depend on the type of the work, they are usually quite low in the domain of authors' rights due to the lack of hindrances to the creation of analogous works by other persons. The invention costs are also quite small.

Clearly, in the framework of this model, putting AI-generated intellectual works in the public domain would not lower societal costs but only discourage persons from applying artificial intelligence.

Conclusion

Our analysis of existing models has shown that, their diversity notwithstanding, only a few of these models stimulate the creation and use of new intellectual works. The most promising model seems to be vesting the rights to an AI-generated work in the organizer of the process of its creation.

Rights to AI-generated works should be more limited than traditional exclusive authors' rights so as to protect the interests of human authors.

In this case, any person who is professionally involved in the creation of IP shall have a choice: using AI to create an intellectual work at a lower

cost while getting a fairly limited right for a relatively short period of time or paying more for the creation of an intellectual work by a human author while getting rights for a longer period. One can surmise that, over time, consumers will increasingly value intellectual works made by human beings (similarly to the value assigned today to unique and hand-made goods).

For this reason, one should make it obligatory for producers to designate whether AI was used to make an intellectual work. This will allow consumers to choose between books and films made by human beings and machines.

In conclusion, we should note that it is pointless to vest AI applications with rights today. At the same time, it appears highly promising to attribute rights to the organizer of the use of AI for the creation of intellectual works. Nevertheless, such a model is not totally new to IP law (it suffices to recall the rights of phonogram producers, broadcasting and cablecasting organizations, and database creators). Thus, the inclusion of artificial intelligence into the IP domain does not require reconstructing the legal framework but only adapting existing approaches.

References

Bently L., Sherman B. (2004) *Intellectual property law*. Oxford: University, 1131 p.

Butler T. (1982) Can a computer be an author: Copyright aspects of artificial intelligence. *Hastings Comm & Ent.,* no 4, pp. 707–747.

Dozortsev V.A. (2003) The right to a film as a complex multilevel work. In: Intellectual Rights: Terms. System. Aim of Codification. Moscow: Statut, pp.143–170.

Feather J. (2010) The significance of copyright history. In: *Privilege and property: Essays on the history of copyright*. N.Y.: Open Books, pp. 359–368.

Garnett K., James J., Davies G. (1999) *Copinger and Skone James on copyright*. L.: Sweet & Maxwell, 1225 p.

Hristov K. (2020) Artificial intelligence and the copyright survey. Available at: https://ssrn.com/abstract=3490458 or: http://dx.doi.org/10.2139/ssrn.3490458 (accessed: 1.02.2021)

Jaszi P. (1992) On the author effect: Contemporary copyright and collective creativity. *Cardozo Arts and Entertainment Law Journal*, no 2, pp.293–320.

Kalyatin V.O. (2016) Defining public domain in contemporary information society. *Pravo. Zhurnal Vysshey shkoly economiki*, no 2, pp. 4–14 (in Russian)

Karapetov A.G. (2016) *Economic analysis of law.* Moscow: Statut, 528 p. (in Russian)

Kreutzer T. (2008) The model of German copyright law and regulation alternatives. Available at: https://www.nomos-elibrary.de/10.5771/9783845212197.pdf?download_full_pdf=1 (accessed: 2.02.2021)

Kumar S., Lavery N. (2019) Does AI generated work give rise to a copyright claim? Available at: https://www.natlawreview.com/§/does-ai-generated-work-give-rise-to-copyright-claim (accessed: 1.02.2021)

Morrigi A. (2017) The role of intellectual property in the intelligence explosion. Available at: https://www.4ipcouncil.com/application/files/9615/1638/1031/The_Role_of_Intellectual_Property_in_the_Intelligence_Explosion.pdf. (accessed: 1.02.2021)

Nazarov N. (2020) Attribution of authorship to intellectual works generated by artificial intelligence. *Intellektual'naya sobstvennost'. Avtorskoe pravo i smezhnye prava*, no 3, pp. 53–62 (in Russian)

Naumov V.B., Tytyuk E.V. (2018) Legal status of the "creative" work of artificial intelligence. *Pravovedenie*, no 3, pp. 531–540 (in Russian)

Perri M., Margoni T. (2010) From music tracks to Google maps: Who owns computer-generated works? *Computer Law and Security Review*, no 6, pp. 621–629.

Prange D., Lawson A. (2018) Re-evaluating companies' AI protection strategies. *Managing Intellectual Property*, no 272, pp. 35–38.

Rai A. (1999) Regulating scientific research: Intellectual property rights and the norms of science. *Northwestern University Law Review,* no 1, pp. 77–152.

Samuelson P. (1986) Allocating ownership rights in computer-generated works. *University of Pittsburgh Law Review*, vol. 47, pp.1185–1204.

Searle J. (1980) Minds, brains, and programs. *Behavioral and Brain Sciences*, no 3, pp. 417–424.

Selvadurai N., Matulionyte R. (2020) Reconsidering creativity: Copyright protection for works generated using artificial intelligence. *Journal of Intellectual Property Law & Practice*, no 7, pp. 536–543.

Solum L. (1992) Legal personhood for artificial intelligences. Available at: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?§=3447&context=nclr (accessed:1.02.2021)

Vaver D. (1994) Translation and copyright: A Canadian focus. *European Intellectual Property Review*, no 4, pp.159–166.

Yu R. (2017) The machine author: what level of copyright protection is appropriate for fully independent computer-generated works? *University of Pennsylvania Law Review*, no 165, pp. 1266–1268.

Electronic interaction and digital technologies in corporate governance of a joint stock company in Russia

Alexander V. Gabov

Chief Researcher, Doctor of Juridical Sciences, Corresponding Member of the Russian Academy of Sciences, Institute of State and Law, Russian Academy of Sciences. Address: 10 Znamenka Str., Moscow 119019, Russian Federation. E-mail: gabov@igpran.ru

Abstract

The article is devoted to key issues in the development of legal regulation of electronic forms of interaction between participants in corporate relations in Russia. The author consistently examines the development of legislation and the practice of its application since the mid-1990 s. until now. The impact of the emergency legislation created to counter the spread of coronavirus infection in 2020 is separately considered. The author analyzes in detail the materials of the Bank of Russia, various political attitudes. For the first time in special literature, the correlation of the development of electronic forms of interaction in private and public relations is shown. The main current legislative initiatives are considered. The purpose of the study is to formulate the main directions of the development of legal regulation, based on the analysis of the experience of the development of legislation, including regulating public relations. To implement this, the first part of the study (introduction) shows the traditional approach to corporate actions, evaluates its pros and cons; then the second part of the study shows the first attempts in the 2000 s. include elements of electronic interaction in regulations; then (in the third part) a radical change in the legislator's approaches to regulation in 2010 is shown, estimates are given of the state of regulation for the period from late 2019 to early 2020 (before the start of the coronavirus pandemic); in the fourth part of the assessment of current draft laws, as well as the author's proposals in terms of directions of regulation are formulated. Based on the results of the work done, the main conclusion was made about the need to expand the use of electronic forms of interaction for all legal entities, as well as the correlation of private law and public law regulation.

Keywords

corporate governance; joint-stock company; proxy voting; electronic voting (e-voting; i-voting; e-proxy voting); remote voting; ballot paper; shareholders' rights; coronavirus infection; restrictions.

For citation: Gabov A.V. (2021) Electronoc interaction and digital technologies in corporate governance of joint-stock company in Russia. *Legal Issues in the Digital Age,* no 1, pp. 64–99.

DOI: 10.17323/2713-2749.2021.1.65.99

The modern Russian legislation on joint stock companies (Federal Law of December 26, 1995 No. 208-FZ "On Joint Stock Companies") in its original version did not provide for the possibility of using electronic communications for interaction between a joint stock company and a shareholder, for counting shareholders' votes; similarly this concerned relations within the collegial bodies of the joint stock company (board of directors, management board and other collegial bodies).

The Law on Joint Stock Companies in a part concerning the meeting of shareholders of a joint stock company provided a traditional form of holding a general meeting in the form of "joint presence" (Articles 50, 55); where personally present shareholders or their representatives could vote by show of hands (i.e., the expression of will was carried out openly) or by filling out ballots with pre-posed questions and dropping such ballots into boxes for their subsequent transfer to the counting commission (i.e., secret ballot) . Such a joint meeting required a special room in which the shareholders and their representatives gathered, a system for their registration, and certain rules for holding the meeting.

This traditional way of holding a general meeting of shareholders had its advantages — first of all a personal contact between shareholders and managers of joint-stock companies.

However, it also had its drawbacks. The main one is the significant expenses of the joint-stock company for holding a meeting (rent, payment of postage and other expenses); for shareholders who were not at the place of the meeting, this method of holding meant the cost of arriving at the place of the meeting.

Problems could arise with voting by filling out ballots, which, if incorrectly formatted, could be invalidated.

Another drawback of a meeting in the form of joint presence is the possibility of various kinds of manipulations with the access of a shareholder or his representative to the venue or, on the contrary, creating a situation that entails the need to remove a shareholder (representative) from the meeting, with the subsequent use of this fact to put pressure on the joint-stock company [Sychev P.G., 2011].

A similar method — referred to as "meeting" (*zasedanie*) — was envisaged as a form of activity of the board of directors (Article 68 of the Law on Joint Stock Companies) and the collegial executive body of the Joint Stock Company (Article 70 of the Law on Joint Stock Companies).

In addition to joint presence, the Law on Joint Stock Companies provided another form of decision-making by the general meeting of shareholders (as a body of the joint stock company) — by absentee ballot, carried out by sending ballots to the address of the joint stock company. In Anglo-American law, this form is called voting by mail ("distance voting") [Kraakman P. et al., 2017: 58].

A similar form of decision-making — absentee ballot — was envisaged for decision-making by the board of directors of a joint-stock company (Article 68 of the Law on Joint-Stock Companies). At the same time, it should be noted that the procedure for such decision-making could be established by an internal local act of the joint-stock company; accordingly, for this body, absentee voting forms could be more flexible (for example, a paper form might not be used).

1. The first attempts to include the elements of electronic interactions in legal regulation

For the first time, the possibility of using electronic tools of communication for the exchange of messages between a shareholder and a joint-stock company, as well as between members of other management bodies between themselves and a joint-stock company, was indicated in the Corporate Code of Conduct.[1]

Firstly, the Code of Corporate Conduct recommended (clause 1.1.3) to include in the charter of a joint-stock company a possibility of using an electronic form of notification of a general meeting as an additional way of notifying shareholders about a general meeting. What was meant by the "electronic form of the message" — the document has not disclosed.

Secondly, the document recommended (clause 1.3.5) to provide shareholders with an additional opportunity to get acquainted with information about the meeting of shareholders through electronic means of communication, including the Internet. In addition to referring to such means the Internet, no other details of what is meant by "electronic means of communication" were given.

[1] Order of the Federal Commission for the Securities Market of Russia. April 4, 2002 No. 421. "On Recommendations for the Application of the Corporate Code of Conduct".

Thirdly, in the part concerning the organizing the activities of the board of directors (supervisory board), the Corporate Code of Conduct recommended (clause 4.5.3) to provide in the internal documents the most acceptable form of notification of the meeting and the procedure for providing information (including by post, telegraph, teletype, telephone, electronic or other communication).

The last two recommendations from the point of view of their implementation (despite the remarks noted above) did not raise questions: in fact, there was no problem in posting information about the meeting of shareholders on the Internet, as well as fixing the provision that notifications and materials for the meeting are sent to a member of the board of directors through various means of communication.

However, the implementation of the first recommendation was associated with difficulties. They were created by the lack of clarity about what the "electronic form of communication" is. In addition, even if such a concept would be disclosed in the internal documents of a joint-stock company, a problem still arose: to implement this method of notification, at least a shareholder's special capabilities (e-mail, fax, etc.) were required; even the posting of relevant information on the Internet at that time (2002) could have had no meaning for a large group of shareholders — elderly individuals who became shareholders following the privatization of the early 1990s. Note also that in the Law on Joint Stock Companies this method of communication — electronic — was not provided.[2] Electronic exchange between a shareholder and a joint-stock company was not regulated in a special way at all.[3]

Nevertheless, in the same 2002 the Federal Commission on Securities Market (FCSM) (Regulation on additional requirements for the procedure for preparing, convening and holding a general meeting of shareholders)[4]

[2] For example, the word "electronic" (as applied to mail) first appeared in the Law on Joint Stock Companies in 2008, when Art. 15 of the Law, a provision was introduced that in the notification of the reorganization of a joint-stock company, "e-mail addresses" could be additionally indicated for communication with the company. In 2009 (Federal Law No. 352-FZ of December 27, 2009, a similar rule appeared in Article 30 of this Law in terms of requirements for reporting a decision to reduce the authorized capital and Article 35 in terms of requirements for the content of a notice of cost reduction net assets.

[3] Such an exchange (between the depositary and the depositor) was mentioned only by the Regulations on depository activities in Russia, approved by the Federal Commission for the Securities Market. October 16, 1997. No. 36, and only in the form of a blanket norm ("acceptance of documents in electronic form as instructions is allowed if this is provided for by the legislation of the Russian Federation or by agreement of the parties").

[4] Order of the Federal Commission for the Securities Market of Russia. May 31, 2002 No. 17.

in terms of additional requirements for the procedure for preparing a general meeting of shareholders (clauses 2.1, 2.4) determined that in the case of if it is provided for by the charter, proposals on the inclusion of issues in the agenda and proposals on the nomination of candidates to the governing bodies and other bodies of the joint-stock company may be made, and the requirements for an extraordinary general meeting may be submitted by electrical communication, for example, by e-mail using electronic digital signature.[5]

As can be clearly seen, mentioned Regulation of the Federal Commission for the Securities Market of Russia went much further than the Corporate Code of Conduct — it was possible for a joint-stock company to establish (without confirmation in paper form with original signatures and seals) an electronic exchange of separate (three types) legally significant messages.

Between the two documents — the Code of Corporate Conduct and the aforementioned FCSM Regulations of 2002 — in the absence of uniformity in terminology, however, there was an important common point: the issue of using electronic communications to interact with shareholders was left to the discretion of the joint-stock company itself; the documents did not contain detailed regulation.

Thus, the issue of the use of electronic interaction technologies, obviously, was on the periphery of the legislator's attention, and was not in any way significant.

This moment reflected the underdevelopment of electronic document management (here we use this term in a broad sense) at that time, the impossibility of including all shareholders in such interaction (as for shareholders — individuals, such a goal was simply unattainable).

This also reflected, in general, some distrust of document management using various electronic means, which was noted later in various policy documents.

So, in 2010, in the State Program "Information Society (2011–2020)",[6] it was noted that "in economic life, electronic forms of interaction have not

[5] Similar regulation was reproduced in 2012 in the new Regulation on additional requirements for the procedure for preparing, convening and holding a general meeting of shareholders, approved by order of the Federal Financial Markets Service. February 2, 2012 No. 12-6 (clauses 2.1, 2.4, 2.5).

[6] Approved by the order of the Government of the Russian Federation of October 20, 2010 No. 1815-r.

yet received proper development, including due to a lack of confidence in their safety and security of information, distrust of electronic payments".[7] Six years later, in 2016, the Bank of Russia stated that[8] "one of the main obstacles to the development of electronic interaction is a psychological or behavioral barrier, largely due to the ignorance of citizens about the possibility of using paperless methods of performing certain financial transactions, as well as distrust of new forms of interaction".[9]

2. Regulatory changes in the 2010s: from personal participation to electronic telecommuting

The 2010s are a period when a radical (although not abrupt) change in the situation with electronic exchange of information is taking place, mainly in the relationship between a shareholder and a joint-stock company.

These changes fully corresponded to the goals and objectives that were set by the state at that time in terms of the accelerated development of electronic forms of interaction in all spheres of the economy. For example, the aforementioned State Program of the Russian Federation "Information Society (2011 — 2020)" as one of its results directly named "interaction of citizens, organizations and public authorities, mainly in electronic form." It should be noted that by this time the practice of using electronic voting in elections both in Russia and abroad had accumulated, which has fully proved its effectiveness [Kersting N., 2007;]; [Pavlushkin A.V., Postnikov A.E., 2009]; [Antonov Ya.V., 2015]; [Tsaplin A.Yu., 2016]; [Matrenina K.Yu., 2017]; [Fedorov V.I., 2017]; [Zakuskin A.A., 2019]; [Khamutovskaya S., 2019]; [Alekseev R.A., Abramov A.V., 2020]; [Kolyushin E.I., 2020]; [Fedorov V.I., 2020].

These changes also took into account the tendencies in the regulation of electronic voting that existed in European practice. For example, in the European Union (in particular, see: Directive 2007/36 / EU of the European Parliament and the Council of 11 July 2007 on the exercise of certain rights

[7] Also see: Federal Target Program "Electronic Russia (2002 — 2010)" (one of its latest editions), approved by the Government of the Russian Federation on January 28, 2002 No. 65.

[8] In the Guidelines for the Development of the Financial Market of the Russian Federation for the Period 2016–2018, approved by the Board of Directors of the Bank of Russia on May 26, 2016.

[9] See: Main directions of development of the financial market of the Russian Federation for the period 2016–2018. Approved by the Bank of Russia Board of Directors. May 26, 2016. Available at: https://cbr.ru/Content/Document/File/44188/onrfr_2016-18.pdf (accessed: 7.02. 2021)

of shareholders in listed companies[10] and Directive (EU) 2017/828 of the European Parliament and the Council of 17 May 2017 amending Directive 2007/36 / EC as regards the encouragement of long-term shareholder engagement[11]), as well as in the United States.[12] Directive 2007/36 / EU, for example, stated that companies should not face legal obstacles in offering their shareholders any means of electronic participation in the general meeting, and voting without personal participation in the general meeting, be it absentee or electronic, should not be subject to restrictions other than those necessary to verify identity and ensure the security of electronic communications.[13]

In 2011 Russia adopted a law that played an important role in the development of electronic forms of interaction between shareholders and joint stock companies (see below) — Federal Law No. 414-FZ of December 7, 2011 "On the Central Securities Depository". This law established (Art. 12) that the Central Securities Depository, its clients (depositors), as well as the persons maintaining the register are obliged to exchange information and documents in electronic form when interacting with each other.

The most significant changes in attitudes towards the electronic exchange of information between a shareholder and a joint stock company at the political and legal level took place in 2013. The action plan ("road map") "Establishing an international financial center and improvement of the investment climate in the Russian Federation",[14] in the section on corporate governance,[15] included a special para 44: "Regulation of electronic methods of interaction between shareholders and a joint stock company." According to this paragraph, it was envisaged in 2014 to establish legal norms (to develop a draft federal law and other legal acts[16]) "regulating

[10] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0036& from=EN (accessed: 1.03.2020)

[11] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0828& from=EN (accessed: 1.03.2020)

[12] Available at: https://ssrn.com/abstract=1731362 (accessed: 1.03.2020)

[13] "Companies should face no legal obstacles in offering to their shareholders any means of electronic participation in the general meeting. Voting without attending the general meeting in person, whether by correspondence or by electronic means, should not be subject to constraints other than those necessary for the verification of identity and the security of electronic communications".

[14] Approved by the order of the Government of the Russian Federation of June 19, 2013 No. 1012-r.

[15] "V. Corporate governance and enforcement, including investor protection, insolvency resolution, contract execution, financial market dispute resolution."

[16] That is, initially it was supposed to have two levels of regulation — legal and sub-legal.

electronic means of interaction between shareholders and the company." Such an impulse was fully consistent with a significant change in public attitudes towards electronic forms of interaction — the availability of the Internet, the prevalence of electronic devices has sharply increased, the composition of shareholders has changed qualitatively.[17]

It should be noted para 44 of the Action Plan "Establishing an international financial center and improving the investment climate in the Russian Federation" was not implemented — a special law on its implementation was never adopted. However, in 2014, the Federal Law of July 21, 2014 was adopted,[18] which supplemented the Federal Law "On the Securities Market" with a special article 8.8 "Specifics of participation in the general meeting of persons whose rights to securities are accounted for by a nominal holder".

According to this article, the following rules of electronic interaction were established in preparation for a general meeting of shareholders with the participation of an issuer (joint-stock company), a shareholder, a nominee holder, a registrar, a central depository [Chekhovskaya S.A., 2016: 77], as well as a voting procedure (the first Russian version of a mechanism long known in Western countries, designated in literature by the term "e-proxy voting") [Novoselova L., Medvedeva T., 2017] ; [Kraakman R. et al., 2017].[19]

The main provisions of the mentioned law are as follows:

the owner of the securities, as well as any other person who, in accordance with federal law, exercises the rights to securities, the rights to which are accounted for by the nominal holder, received the right to take part in

[17] During this period, there are also rare works in which attempts are made to assess the possibility of using electronic technologies in the implementation of corporate actions [Druzhinin A., 2012].

[18] Judging by the text of the explanatory note to the draft Federal Law No. 359513-6 "On Amendments to Certain Legislative Acts of the Russian Federation in Connection with the Adoption of the Federal Law" On Guaranteeing the Rights of Insured Persons in the System of General Pension Insurance of the Russian Federation in the Formation and Investment of Pension Savings Funds the corresponding changes were not planned initially. This is understandable — it is clear from the title that the document was originally developed for completely different purposes. According to the Table of amendments to the draft federal law No. 359513-6, recommended by the Committee on the Financial Market for adoption during the consideration of the draft in the second reading, the corresponding changes — the introduction of Art. 8.8 to the Law on the Securities Market — were proposed by the deputy of the State Duma Natalia Burykina.

[19] In fact, the first Russian version of voting with the participation of intermediaries, which is known in foreign practice as "proxy voting" or "proxy voting through custodial institutions or other intermediaries".

the general meeting of the owners of securities by giving instructions[20] to the nominal holder to vote in a certain way; such a right could arise only if it was provided by an agreement with a nominee holder;

the issuer of securities, if a personal account of the nominal holder of the central securities depository has been opened in the register of securities holders, — must ensure that securities holders can participate in the general meeting by sending an electronic document signed with an electronic signature;

the registrar is obliged to send the information contained in the voting ballot to the central securities depository and the nominal holder registered in the register of securities holders in the form of an electronic document signed with an electronic signature;

the voting document containing the information required by law[21] was formed by the nominee holder on the basis of instructions received from the owner of the securities. The nominee holder sent the voting document to the registrar, and if such a nominee holder is a depositor of another nominee holder, to such a nominee holder. The voting document was signed with an electronic signature.

The main problem of the new regulation was the lack of corresponding provisions ensuring the real "functioning" of the e-proxy voting mechanism in the legislation on joint stock companies.[22]

In addition to the Law of July 21, 2014 No. 218-FZ, another document appeared in 2014, which described a recommendation on the use of document automation between a shareholder and a joint stock company — the Corporate Governance Code (Information Letter of Bank of Russia of April 10, 2014 No. 06-52 / 2463), which replaced the 2002 Corporate Code of Conduct.

---

[20] Literally, the norm looked like this "personally or by giving instructions"; it is difficult to say why it was formulated in this form, since this article is clearly not a suitable place to describe such a fundamental issue as the right to participate in the general meeting of securities holders.

[21] The voting document must contain information on the owners of securities and on other persons who, in accordance with federal law or personal law, exercise the rights to securities, on the number of securities owned by such persons, as well as the results of their voting on each item on the agenda of the general meetings of owners of securities.

[22] It should be noted that in the 2014 report of the Bank of Russia "Barriers to the development of electronic interaction in the financial market" it was stated that "in the field of corporate relations, a significant gap is the lack of a legislative framework for creating an electronic system of interaction between shareholders and a joint-stock company" Available at: https://cbr.ru/finmarkets/files/interaction/1a.pdf (accessed: 1.03.2021)

In accordance with the 2014 Corporate Governance Code (currently in force), the following recommendations are provided:

the notice of the general meeting and materials thereto are sent to shareholders, whose rights are recorded by depositories (nominee holders) in electronic form;

joint stock companies were recommended to provide an opportunity for shareholders, whose rights are recorded in the register, to receive a notification about the meeting and have access to the meeting materials in electronic form at request of a shareholder;

joint-stock companies were advised, in addition to posting on the Internet a message about the upcoming general meeting of shareholders, to post materials for the meeting in question on their websites;

joint-stock companies were recommended, taking into account the technical capabilities, "to strive to create a convenient procedure for shareholders to send to the company requests to convene a general meeting, proposals for nominating candidates to the company's bodies and making proposals to the agenda of the general meeting"; while and it was recommended "to use modern means of communication and provide the exchange of information in electronic form";

joint-stock companies were recommended to "create systems, taking into account the technical conditions, allowing shareholders to take part in voting using electronic means". In particular, it was recommended "in order to create the most favorable conditions for the participation of shareholders in the general meeting, provide for the possibility of filling out a voting ballot in electronic form, for example, through a personal account on the company's website on the Internet, provided that sufficient security and protection is ensured, as well as accurate identification of persons, taking part in the meeting";

joint-stock companies with a large number of shareholders were advised to use telecommunications to ensure remote access of shareholders to the general meeting (for example, to broadcast the general meeting of shareholders on the website of the joint-stock company on the Internet, use video conferencing);

to implement the principle of accessibility of disclosed information, joint stock companies were recommended to use a variety of channels and methods of disclosing information, primarily electronic, accessible to the majority of interested parties;

joint-stock companies were recommended "taking into account ... technical capabilities ... to strive to create a convenient procedure for shareholders to send requests for access to information and documents of the company (in particular, to regulate the use of modern means of communication and exchange of information in electronic form)";

joint stock companies were recommended to provide information and documents to shareholders "in a way convenient for shareholders and in a form appropriate for them, including using electronic media and modern means of communication (taking into account the wishes of those who sent the request to provide documents to the form of their provision and the method of their delivery)".

The implementation of these recommendations was complicated by the lack of legislative regulation of electronic interaction. The Bank of Russia, in its Review of Corporate Governance Practices in Russian Public Companies, prepared on the basis of public data disclosed by companies in their 2015 annual reports, noted that "most companies ... are experiencing difficulties ... with the provision of electronic means of remote access to shareholders' meetings ..."[23]

It was recommended to use electronic forms of interaction when interacting with members of boards of directors (supervisory boards), namely, it was recommended:

"to fix in internal documents the provision that when holding meetings of the board of directors in person, to determine the presence of a quorum and voting results, a written opinion on the agenda of a meeting of a member of the board of directors who is absent from the meeting is taken into account. It is necessary to determine the procedure for obtaining a written opinion from a member of the board of directors, ensuring its prompt direction and receipt (for example, by telephone or electronic communication)";

to provide in the internal documents "a form of notification of a meeting and a procedure for sending information, ensuring its prompt receipt (including via electronic communication), most acceptable for members of the board of directors."

In 2015, the G20 / OECD Principles of Corporate Governance appear. This document:

[23] See: Overview of corporate governance practices in Russian public companies based on disclosed by companies in 2015 annual reports, P. 17. Available at: http://www.cbr.ru/collection/collection/file/24046/review_17042017.pdf (accessed: 7.02.2021)

welcomes — as a measure "to remove artificial barriers to participation in general meetings of shareholders" — to encourage the use of "electronic absentee voting, including the submission of electronic materials and reliable systems of confirmation of votes";

notes the need for widespread use of "information technology in the voting process, including secure electronic voting in all public companies."[24]

In 2015 a document was adopted that was not directly aimed at expanding the electronic interaction of participants in corporate governance, but had an impact on their development — the Action Plan for the development of electronic interaction in the financial market.[25] Among the goals of this document there were such as "consistent reduction of paper workflow in the financial market", as well as "creation of prerequisites for the refuse of paper workflow in the financial market."

The apogee in the development of electronic methods of interaction of a joint-stock company with shareholders in the 2010s was adoption of the Federal Law of June 29, 2015 No. 210-FZ,[26] as a result:

the e-proxy voting mechanism has been changed. In particular, Art. 8.8 of the Law on the Securities Market ceased to be in force. A new article was introduced into the Securities Market Law — Article 8.9. Specifics of the exercise of rights to securities by persons whose rights to securities are accounted for by a nominal holder.

If earlier Art. 8.8 of the Law on the Securities Market was the only rule describing the e-proxy voting mechanism, then Art. 8.9 of the Law on the Securities Market (after the adoption of Law No. 210-FZ dated June 29, 2015) has become only a part (albeit an important one) of this mechanism.

This article provides[27] that the person exercising the rights to securities (shareholder), if the rights to them are accounted for by the nominee holder, is entitled by giving instructions:[28]

---

[24] Available at: https://www.oecd-ilibrary.org/docserver/9789264252035-ru.pdf?expires= 1611827492&id=id&accname=guest&checksum=23DA6A3733B03278B2653E-853207C9A5 (accessed: 7.02.2021)

[25] Available at: http://static.government.ru/media/files/woFl5dADTluVf5jIgAmGI0vbegU74awz.pdf (accessed: 7.02.2021).

[26] This bill was not aimed directly at the development of electronic document management.Available at: https://sozd.duma.gov.ru/bill/469229-5 (accessed 7.02.2021)

[27] If it is provided by the contract of the person with such an organization.

[28] According to this article, the procedure for giving instructions is determined by an agreement with these organizations.

to propose agenda items for the general meeting of securities holders;

to nominate candidates to the governing bodies and other bodies of the joint stock company;

to demand the holding of a general meeting of owners of securities;

to take part in the general meeting of owners of securities and exercise the right to vote;

Organizations, having received instructions, send an e-message containing the expression of the will of the person exercising the rights to securities to the person with whom an agreement has been concluded on opening a personal account (depo account) of a nominee holder.

To exercise the right under Art. 8.9 of the Law on the Securities Market, in accordance with the amendments made to Art. 60 of the Law on Joint Stock Companies, receipt by the registrar of a joint stock company of messages on the will of persons who:

have the right to participate in the general meeting of shareholders;

are not registered in the register of shareholders of the joint stock company;

gave instructions on voting to the persons registering their rights to shares;

is equivalent to voting by ballots.

At the same time, according to the changes in Art. 58 of the Law on Joint Stock Companies, shareholders who have given instructions on voting to persons registering their rights to shares are considered to have taken part in the general meeting of shareholders if notifications of their will are received no later than two days before the date of the general meeting of shareholders or until the deadline for admission ballots when holding a general meeting of shareholders in the form of absentee voting;

the forms and methods of communicating information about the meeting to the persons registered in the register have changed significantly:

the Law on the Securities Market was supplemented with a new article 30.3, according to which the issuer is obliged to provide information related to the exercise of rights on securities to the central securities depository, if a personal account of the nominal holder of the central depository is opened for him in electronic form in the manner and formats established by the central depository;

Art. 52 of the Law on Joint Stock Companies was supplemented with an indication that the charter of a joint stock company may provide for other methods of communicating information about the holding of a meeting, except for sending registered letters or handing over against signature. It is now allowed to specify the following methods in the charter:

sending an electronic message to the email address indicated in the register of shareholders of the company and / or;

sending a notice of the general meeting of shareholders to the contact phone number or e-mail address, which are indicated in the register of shareholders of the company and / or;

publication in a print form specified in the charter of the company and / or posting on a website specified in the charter of the company;[29]

provides the possibility of electronic registration for participation in the meeting of shareholders — Art. 58 of the Law on Joint Stock Companies indicates that the following are considered to have taken part in the general meeting of shareholders;

shareholders who have registered to participate in it, including on the website specified in the announcement of the general meeting;

shareholders whose electronic ballot papers are filled out on the specified website no later than two days before the date of the general meeting of shareholders. To fill out the electronic ballot on the indicated website, Art. 54 of the Law on Joint Stock Companies provides that in preparation for such a meeting, the board of directors of a joint stock company must determine the address of the website, where the electronic form of ballots can be filled out;

the procedures for remote interaction during voting have been regulated (from the moment the ballot is sent to the shareholder and until it is received back by the joint stock company), namely:

Article 49 of the Law on Joint Stock Companies has been supplemented with a separate clause 11, according to which, during an in-person meeting of shareholders, communication technologies can be used to ensure the possibility of remote participation of shareholders to discuss agenda

[29] Let's note that some researchers, pointing out the limited use of other electronic technologies, explain this by the fact that "there is no contractual relationship between the registrar and the persons registered in the register, while any use of electronic documents when providing information to shareholders requires the conclusion of a separate agreement for the purpose of giving legitimacy to these electronic documents "[Medvedeva T.M., Azimova L.V., 2020: 66–67].

items and make decisions on issues put to a vote without being present at place of the meeting. This rule, in essence, is an attempt to transfer the provisions of the 2014 Corporate Governance Code into federal law. This attempt cannot be recognized as fully successful — this rule does not agree with other provisions of the Law on Joint Stock Companies (even terminologically). It should also be noted that the wording of the above rule clearly excludes the possibility of holding a meeting with remote electronic participation of all shareholders (or their representatives) [Medvedeva T.M., Azimova L.V., 2020: 72];

according to the changes in Art. 60 of the Law on Joint Stock Companies, the charter of a joint stock company *may provide for the sending of a voting ballot in the form of an electronic message to the email address specified in the register of shareholders of the company when holding a general meeting of shareholders*:

in the form of absentee voting;

in a public joint stock company;

in a non-public joint stock company with the number of shareholders — owners of voting shares of 50 or more;

in another company, the charter of which provides for the mandatory sending or delivery of ballots before the general meeting of shareholders.

To implement the possibility of sending a ballot to the shareholder in electronic form: Art. 54 of the Law on Joint Stock Companies provides that in preparation for the general meeting of shareholders, the board of directors (supervisory board) is obliged to determine: the form and text of the voting ballot in case of voting by ballots, the wording of decisions on the agenda items of the meeting, which must be sent in electronic form by nominal holders registered in the register of shareholders; according to Art. 52 and 54 of the Law on Joint Stock Companies, in preparation for the general meeting of shareholders, the board of directors (supervisory board) is obliged to determine the e-mail address to which the completed ballots can be sent (Article 54), which must be indicated in the subsequent notice of the general meeting shareholders (Article 52);

a separate mechanism for electronic voting using the Internet ("e-voting")[30] has been introduced. The basis of this mechanism is set forth in

[30] Here it is necessary to make terminological clarifications. We see the use of the term "e-voting" to describe electronic voting in a number of modern works [Magdalinskaya Yu.V., 2020]. However, in a number of cases, when the authors want to emphasize the remote nature of electronic interaction, a different term is introduced — "i-voting" [Ba-

paragraph 4 of Art. 60 of the Law on Joint Stock Companies, which stipulates that the charter of a joint stock company may provide a filling out an electronic form of ballots on a website, the address of which is indicated in the notice of the general meeting of shareholders. However, from a legal point of view, these prescriptions are presented in an extremely careless manner; they make up the second sentence of this paragraph (the paragraph consists of four sentences in total), which looks like a separate norm that does not create unity with the first sentence, which has nothing to do with the e-voting mechanism at all.[31]

To implement the e-voting mechanism, Art. 54 of the Law on Joint Stock Companies provides that the board of directors (supervisory board) of a joint stock company is obliged to determine the address of the, where the electronic form of ballots can be filled out; Art. 52 of the Law on Joint Stock Companies indicates that the notice of the general meeting must indicate the address of the site on which the electronic form of ballots can be filled out, if such a method of filling out ballots is provided for by the charter of the joint stock company. It should be noted that these legal norms do not directly specify which websites are in question, i.e., when adopting the relevant provisions, the legislator adhered to a dispositive approach;

Art. 60 of the Law on Joint Stock Companies provides that filling out the electronic form of ballots on the website can be carried out by shareholders during the general meeting of shareholders, if they have not exercised their right to participate in such a meeting in another way. At the same time, it is not indicated that this possibility exists only if such a form of electronic voting is provided for by the charter, but, apparently, this is still one of the conditions for using such an option, although the law could have indicated this more clearly;

---

taeva B.S., 2020: 76]. The appearance of the latter term is not accidental, the fact is that the special literature on the use of electronic methods of expression of will in the electoral process indicates the differences between "e-voting" and "i-voting". The first is understood as "voting at stationary polling stations" ", but the second is actually" remote voting with the help of technical devices "[Fedorov V.I., 2020: 35].

[31] An attempt to make such a "bundle" was made by the Bank of Russia in a letter dated May 27, 2019 No. 28-4-1 / 2816, that "within the meaning of paragraph 4 of Article 60 of Law No. 208-FZ, filling out an electronic form of ballots by a person entitled to participate in the general meeting of shareholders, on the website, the address of which is indicated in the notice of holding the general meeting of shareholders, can only be provided for by the charters of companies that send or deliver ballots, or publish ballots in accordance with paragraphs 2 and 3 of Article 60 of Law No. 208-FZ " ... Such an explanation has already received well-deserved criticism in doctrunee, where it is noted that such an interpretation significantly narrows the possibilities of holding general meetings using electronic technologies [Medvedeva T.M., Azimova L.V., 2020: 72].

e) other cases of electronic interaction have been established:

Art. 41 of the Law on Joint Stock Companies was supplemented with a provision stating that an application for the acquisition of the offered securities of a person with a preemptive right may be sent to the registrar of the joint stock company in the form of an electronic document, if this is provided for by the rules for maintaining the register. It is also indicated that such rules may provide for the possibility of signing an electronic document with a simple or unqualified electronic signature;

in Art. 76 of the Law on Joint Stock Companies, an amendment has been made, according to which the requirement to purchase shares of a shareholder registered in the register of shareholders of the company, or the withdrawal of such a requirement is presented to the registrar of the company by mailing or handing over against signature a written document signed by the shareholder, and if this is provided for by the rules on maintaining the register, also by sending an electronic document signed with a qualified or simple electronic signature.

In 2016, the Bank of Russia in the "Main directions of development of the financial market of the Russian Federation for the period 2016–2018" among the measures that should ensure the achievement of the goals set by the document calls "stimulating the use of electronic interaction mechanisms in the financial market."

In 2016, a document was adopted aimed at implementing the amendments made to the Law on the Securities Market in June 2015 in terms of organizing electronic interaction between the issuer, the joint-stock company and the central depository. (Decree of the Bank of Russia. June 1, 2016. No. 546-P "On the list of information related to the exercise of rights on securities provided by issuers to the central depository").

Amendments to the Law on Joint Stock Companies, introduced by the Law of June 29, 2015 No. 210-FZ, in terms of expanding electronic forms of interaction when convening, preparing and holding a general meeting of shareholders, were developed in the Regulation of the Bank of Russia No. 660 of November 16, 2018 -P "On General Meetings of Shareholders".[32] In par-

[32] The Bank of Russia commented on the creation of this document as follows: "Based on new changes in legislation, as well as taking into account changes in the development of information technologies in order to ensure the comfortable exercise by shareholders of their rights, a Bank of Russia normative act has been adopted that establishes additional requirements for the preparation, convocation and holding general meeting of shareholders. The regulatory act defines the specifics of participation in the general meeting of shareholders whose rights to shares are accounted for by a nominee holder, voting by

ticular, in addition to the provisions that retained the previous regulation in relation to electronic interaction, the following important norms appeared:

a proposal for the agenda of the general meeting and the requirement to hold an extraordinary general meeting are recognized as received if they were received from shareholders in the form of an electronic document of a nominee registered in the register of shareholders of the company (para 2.2);

the date of receipt of the proposal on the agenda of the general meeting or the requirement to hold an extraordinary general meeting of shareholders was determined, including if several shareholders act jointly, sent in the form of an electronic document (clauses 2.5, 2.12, 2.13, 2.16, 2.17);

para 2.18 established the possibility of applying the candidate's consent to be nominated to the governing body of the joint-stock company "in the form of electronic images of documents (documents on paper, scanned with preservation of their details)";

para 3.9 establishes the period within which the joint-stock company must send to the registrar the wording of decisions on the agenda items of the shareholders meeting, as well as voting ballots for the purpose of sending them in electronic form to nominees in accordance with the rules established by Art. 8.9 of the Law on the Securities Market;

para 4.3 establishes that if the company's charter provides for the filling out the electronic form of ballots by a person entitled to participate in the general meeting on the Internet site, the website of the joint-stock company itself or its registrar or central depository can be used.[33] As can be seen from the above rule, an act of the Bank of Russia, in contrast to the provisions of the Law on Joint Stock Companies (Article 52.54), restricts sites that can be used in terms of the e-voting mechanism;[34]

---

filling out an electronic bulletin on the Internet, as well as the procedure for jointly exercising by shareholders their rights "(see: Annual report of the Bank of Russia for 2018. App. 04/26/2019, p. 189. Available at: http://www.cbr.ru/collection/collection/file/19699/ar_2018.pdf (accessed: 7.02.2021)

[33] At the same time, as noted in one of the letters of the Bank of Russia, "the specified norm does not exclude the possibility of the simultaneous use for the specified purposes of more than one of the specified sites on the Internet. At the same time, based on clause 4.7 of the Regulations, if the general meeting is held with the possibility of filling out the electronic form of ballots on the website, registration of persons participating in the general meeting in this way is carried out on the website on which the electronic form of the bulletin is filled in "(see: Letter of the Bank of Russia. May 27, 2019. No. 28-4-1 / 2816 // SPS Consultant Plus.

[34] The purpose of such a limitation is not clear, researchers note this approach excludes use of the official sites of depositories — nominal holders [Medvedeva T.M., Azimova L.V., 2020: 73].

para 4.7, 4.8, 4.11 establish the specifics of registration and attendance at the meeting. In particular, para 4.7 establishes the peculiarities of registration of persons participating in the general meeting, if the general meeting is held with the possibility of filling out an electronic form of ballots: registration of persons participating in the general meeting in this way is carried out on a website, where the electronic ballot form is filled out.[35] Para 4.8 determines that persons entitled to participate in the general meeting, whose electronic form of ballots has been is filled out on the Internet no later than two days before the date of the general meeting, have the right to attend the meeting. Para 4.11 defines the specifics of identification, authorization, registration of persons participating in the general meeting without being present at the venue of the meeting with the possibility of filling out an electronic form of ballots on the Internet site;

in accordance with para 4.13, before the beginning discussion on the election of the body of a joint-stock company, whose members are elected by cumulative voting, information on the number of votes cast for each of the candidates elected to the body of the company must be brought to the attention of the persons present at the general meeting of shareholders by cumulative voting, using ballots that have been received or the electronic form of which is filled out on the website, no later than two days before the date of the general meeting;

para 4.33 requires the e-mail address to be reflected in the minutes of the general meeting to which the completed voting ballots were sent during the general meeting both in person and in absentia, if voting on the issues included in the agenda of the general meeting could be carried out by sending it to the company completed ballots. If the general meeting was held with the possibility of filling out electronic ballots on the Internet — also the address of such a site has to be disclosed.

One of the directions for the development of electronic interaction between the joint-stock company and the shareholder was the adoption of the Bank of Russia directive No. 5182-U. June 28, 2019 "On additional requirements for the provision of documents or copies of documents by joint-stock companies." This document (par. 11) provides for the possibility of a shareholder sending a request for information by e-mail, if this is provided for by the charter or internal document of the joint stock company.

The last document in the "pre-COVID" era on issues of interest to us was the decree of the Government of the Russian Federation of January 17, 2020

[35] See also: Letter of the Bank of Russia. May 27, 2019 No. 28-4-1 / 2816.

No. 19-r.[36] With this document, the plan "Transformation of the business climate", adopted in 2019, was supplemented by a provision on the need to prepare proposals (for example, in the form of a report to the Government) on providing "joint stock companies with the opportunity to hold a general meeting of shareholders online, which will allow using electronic services to organize the broadcast of speeches of the company's leaders, ask them questions, declare a quorum and results of absentee voting and carry out a remote vote via the shareholder's personal account.

There is no information on the implementation of this item of the plan in publicly available sources; at the same time, the corresponding item was later not included in the new version of the Action Plan for the implementation of the mechanism for managing systemic changes in the legal regulation of entrepreneurship "Transformation of the business climate", "Corporate governance, special administrative regions, bankruptcy procedure, appraisal activities".[37]

As can be seen from the previous presentation, by the end of the 2010s. a complex of regulatory provisions has developed that regulate the use of electronic means of communication for interaction between a joint-stock company and a shareholder, both directly and through intermediaries — professional participants in the securities market.

This complex was formed under the influence of Russian and Western experience in using electronic technologies in elections, recommendations of international organizations on organizing electronic remote interaction of corporations and their participants, as well as program and other official documents setting goals and objectives in the field of creating electronic government and improving corporate governance.

The aforementioned complex includes provisions constituting legislation on joint stock companies and legislation on the securities market; it is represented by two federal laws (the Law on Joint Stock Companies and the Law on the Securities Market), acts of the Bank of Russia, as well as separate clarifications of the regulatory nature of the Bank.

As a result, in the "pre-COVID" era, new (electronic, remote) forms of interaction between shareholders and joint-stock companies began to be used; the necessary amendments were made to the charters of the largest public joint stock companies; to provide new opportunities, a range of

[36] This document amended the order of the Government of the Russian Federation. January 17, 2019. No. 20-p "On the approval of the plan" Transformation of the business climate.

[37] Approved by order of the Government of the Russian Federation. July 2, 2020. No. 1723-p.

services [Chekhovskaya S.A.,2018] ; [Elnikova E.V., 2020] began to form, created and provided by the central depository,[38] professional participants in the securities market (registrars)[39] and IT companies; the number of shareholders who voted using the Internet grew every year.[40]

There are, nevertheless, some critical comments to this quite favorable view. First, let's note that:

during the specified period, regulation did not develop in terms of the use of electronic forms of interaction in other corporations, as well as in various civil law communities (with rare exceptions);[41]

with the exception of the Corporate Governance Code, no rules have been created for the activities of other collegial bodies of a joint stock company, except for the general meeting of shareholders (board of directors, collegial executive bodies and other bodies).

During this period, the legal regulation of the use of special technical means of counting votes, various electronic forms of interaction between participants in the electoral process (filing an application for inclusion in the voter list at the location via the "Mobile Voter" mechanism, remote electronic voting),[42] as well as meeting participants (including voting) for

[38] Available at: https://www.e-vote.ru/ (accessed: 7.02.2021)

[39] A description of such interaction using the services "personal account of the issuer" and "personal account of the shareholder" on the example of one of the largest Russian registrars JSC "DRAGA" is given in [Lanskov D.P., Danilova S.A., 2019: 14–17].

[40] Complete statistics for Russia does not exist, however, in some works, sample statistics are provided for some of the largest issuers — joint stock companies [Bataeva B.S., 2020: 83].

[41] The exceptions are: - development since 2014 of the institution of absentee voting of owners of premises in apartment buildings using information systems — the state information system of housing and communal services (Articles 44, 44.1, 47.1 of the Housing Code of the Russian Federation. (Federal Law of July 21, 2014 No. 263- Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation in Connection with the Adoption of the Federal Law" On the State Information System of Housing and Communal Services"; Federal Law of June 29, 2015 No. 176-FZ" On Amendments to the Housing Code of the Russian Federation "In this regard, normative acts of the constituent entities of federation were also adopted (for example, the order of the Moscow Department of Information Technologies of February 27, 2018 No. 64-16-87 / 18 "On Approval of the Rules for the Use of the Active Citizen Information System" implementation of the pilot project "Electronic House")); the possibility of using these information systems to manage housing and housing construction cooperatives and homeowners' associations (Articles 113, 135 of the Housing Code of the Russian Federation). However, it is impossible to call such regulation clear, and in relation to the last three indicated subjects, the Housing Code contains only a general indication without any detailed description.

[42] See: Federal Law No. 93-FZ of July 21, 2005 "On Amendments to the Electoral Legislation of the Russian Federation"; Federal Law of May 29, 2019 No. 103-FZ "On the

the defense of dissertations for academic degrees.[43] That is, both the use of special technical means for counting and processing ballots and electronic forms of interaction were in great demand in public relations. However, with all the similarity of the problems being solved (increased activity, cheaper process, etc.), we see no single political and legal attitudes to public and private relations, no single approaches to solving problems (even the terminology used is different).

Secondly, the established regulation cannot be considered optimal:

the technical imperfection of these legal regulations should be noted. They are unnecessarily complicated and do not provide answers to some important questions. This is partly due to the fact that the legislator tried to include electronic forms of interaction in the existing procedural norms of the Law on Joint Stock Companies, without making sseparate articles devoted to that;

the configuration of the specified regulations is not fully optimal (separation of norms between two laws, between a federal law and a decree); noteworthy in this configuration is the presence of clarifications on the part of competent executive body — which is a consequence of the abovementioned technical imperfection of the norms;

the legislator passes over in silence the issues of using electronic technologies for voting by shareholders at the meeting in person, paying special attention only to remote interaction procedures. This idea can be expressed in another way: the legislation on joint-stock companies does not distinguish between cases of using electronic devices for interaction (voting, first of all), which can be at the place of the meeting in person and remote voting using electronic devices.

Experiment on the Organization and Implementation of Remote Electronic Voting at the Elections of Deputies of the Moscow City Duma of the Seventh Convocation"; Resolution of the CEC of Russia. July 6, 2011. No. 19 / 204-6 "On the procedure for using technical means of counting votes — complexes for processing ballots in 2010 at elections and referendums held in the Russian Federation"; Resolution of the CEC of Russia. September 7, 2011. No. 31 / 276-6 "On the Procedure for Electronic Voting Using Complexes for Electronic Voting in Elections"; The procedure for remote electronic voting in the by-elections of deputies of the State Duma of the Russian Federation of the seventh convocation in single-mandate constituencies on September 13, 2020, approved by the decree of the Central Election Commission of July 27, 2020 No. 261 / 1924-7 and a number of other regulations.

[43] Within the framework of local regulations of organizations that have received the right to independently award academic degrees in accordance with Federal Law No. 148-FZ of May 23, 2016 "On Amending Article 4 of the Federal Law" On State Scientific and Technical Policy".

It should also be noted that the dissemination of the new rules proceeded with difficulty, which is clearly seen in the reviews of the corporate governance practice of the Bank of Russia in terms of the recommendations of the 2014 Corporate Governance Code on the need to ensure remote access of shareholders to the shareholders' meeting (principle 1.1.6).

The Review of corporate governance practices in Russian public companies, compiled on the basis of annual reports for 2016,[44] does not provide detailed data, but only notes that the relevant principles turned out to be the most difficult to comply with "as in 2015" (analysis of the 2015 Review, see above).

The Review of Corporate Governance Practices in Russian Public Companies, prepared on the basis of annual reports for 2017,[45] provides a more detailed analysis. In particular, it is noted that the relevant recommendations "are observed only by some companies".[46]

The review of corporate governance practices in Russian public companies for 2018[47], is similar in conclusions to the previous ones — it is also noted that "many companies still use traditional forms and tools for holding general meetings of shareholders". The review discloses the reasons of it.[48] However,

[44] See: Review of corporate governance practices in Russian public companies... P. 16. Available at: http://www.cbr.ru/collection/collection/file/24045/review_27122017.pdf (accessed: 7.02.2021)

[45] See: Review of corporate governance practices in Russian public companies... P. 17–18. Available at: http://www.cbr.ru/collection/collection/file/24044/review_04122018.pdf (accessed: 7.02.2021)

[46] The following reasons for this state of affairs, mentioned by joint-stock companies, were noted: the lack of provisions in the charters on the possibility of remote participation in voting; lack of technical capability for remote voting; impossibility to ensure the identification of shareholders; significant financial costs for the technical support of remote voting; low activity of minority shareholders in general meetings of shareholders over the past years; low level of information literacy and technical skills among certain groups of minority shareholders; the habit of shareholders to take part in a meeting "the old fashioned way" (sending filled-out ballots or attending meetings in person). See: Review of corporate governance practices in Russian public companies (hereinafter referred to as the Review) gor 2018. P. 24. Available at: http://www.cbr.ru/collection/collection/file/25363/review_29112019.pdf (accessed: 7.02.2021)

[47] See: Overview of corporate governance practices in Russian public companies based on 2018 annual reports. P. 24. Available at: http://www.cbr.ru/collection/collection/file/25363/review_29112019.pdf (accessed: 7.02.2021)

[48] "As the reason for the society, they usually cite the insufficient level of information and technical literacy of certain groups of shareholders, the lack of relevant requests from the shareholders. Some companies also cite as reasons for refusing to use telecommunications to provide shareholders with the opportunity to remotely participate in general meetings, the high cost of relevant technologies and services, the lack of technical capacity for the company to implement remote access technologies."

new aspects appear in the position of the Bank of Russia: it notes the need to consider the issues of using telecommunications in order to provide shareholders with remote access on a periodic basis;[49] an interesting "prediction" was made as to why such methods will become more widespread over time: "The composition of the company's shareholders changes over time and a new generation of investors is coming to replace them, for whom remote forms of participation in the meeting may be much more convenient and preferable than traditional ones. In addition, it is necessary to take into account the rapid development of information technology, including the solutions proposed for remote participation in shareholders' meetings".[50]

In the Review for 2019[51] the Bank of Russia notes a positive trend in the implementation of Principle 1.1.6 "over the entire monitoring period". The following is noted: "if at the end of 2015 14 companies (17%) announced the introduction of principle 1.1.6 of the Code into their corporate practice, then in 2019, according to self-assessment, 31 companies (51%) fully comply with this principle, one of the criteria which is the consideration by the board of directors of the issue of providing shareholders with remote access to general meetings."

3. COVID-19 as a trigger for the transition to telecommuting interaction of participants in corporate governance

The rapid and widespread spread of coronavirus infection (COVID-19) both in Russia and around the world has led to the adoption of restrictive

[49] "The annual consideration by the board of directors of the issue of using telecommunications in order to provide shareholders with remote access to participate in general meetings of shareholders is important to create the most favorable conditions for shareholders to exercise their rights. Of course, the board of directors should balance the need to introduce technologies for remote participation in the general meeting of shareholders with both the needs of shareholders and the economic capabilities of the company, but this does not mean that the need to introduce such technologies should not be considered on a periodic basis."

[50] "The Bank of Russia believed that" adherence to principle 1.1.6 of the Code will enable the board of directors to respond in a timely manner to new needs and requests from shareholders, to apply new technologies in the procedures for interacting with them, thereby contributing to the creation of the most favorable conditions and opportunities for shareholders to participate in management society and increasing the attractiveness of society in the eyes of existing and potential investors". See: Overview of corporate governance practices in Russian public companies based on 2019 annual reports. P. 13. Available at: http://www.cbr.ru/collection/collection/file/31741/review_corp_14122020.pdf (accessed: 7.02.2021)

[51] Ibid.

measures by public authorities in many countries. In Russia, restrictions were formed at two levels: federal[52] and regional.[53]

The relevant measures were varied, formulated using different concepts,[54] the main ones of which are:

"ban" (mass events, etc.);

"temporary suspension" (events with full-time attendance; attendance by citizens of public events, etc.);

the imposition of additional responsibilities (use of personal protective equipment; "compliance with the regime of self-isolation"; compliance with measures for "social distancing", etc.);

restriction of movement of citizens;

suspension of the validity of the right ("suspension of the validity of some public transport tickets", etc.).

The restrictions imposed immediately made it clear that corporate actions such as meetings of shareholders in person would be impossible or extremely difficult in a to hold certain period.

The restrictions imposed immediately made it clear that corporate actions such as meetings of shareholders in person would be impossible or extremely difficult in a certain period. To solve the problem, the state was forced to make special legal decisions in the form of extraordinary federal laws;[55]

[52] For example, see: Federal Law of April 1, 2020 No. 99-FZ "On Amendments to the Code of Administrative Offenses of the Russian Federation"; Decree of the President of the Russian Federation of April 2, 2020 No. 239 "On measures to ensure the sanitary and epidemiological well-being of the population on the territory of the Russian Federation in connection with the spread of a new coronavirus infection (COVID-19)"; Decree of the President of the Russian Federation of April 28, 2020 No. 294 "On the extension of measures to ensure the sanitary and epidemiological well-being of the population in Russia in connection with the spread of a new coronavirus infection (COVID-19)"; Presidential Decree of May 11, 2020 No. 316 "On determining the procedure for extending measures to ensure the sanitary and epidemiological well-being of the population in the regions of the Russian Federation in connection with the spread of a new coronavirus infection (COVID-19)."

[53] The most famous example, which served as a benchmark for other regions of Russia, is the Decree of the Mayor of Moscow. March 5, 2020 No. 12-UM "On the introduction of a high alert regime."

[54] In the Presidential Decree of April 2, 2020, they are generally designated as "restrictive and other measures."

[55] For an overview of selected measures, see also the Bank of Russia's Review of Corporate Governance Practices in Russian Public Companies for 2019. P. 8–9. Available at:

Art. 2 of the Federal Law of March 18, 2020 No. 50-FZ "On the acquisition by the Government of the Russian Federation from the Central Bank of the Russian Federation of ordinary shares of the public joint stock company Sberbank of Russia" (hereinafter — the Law of March 18, 2020 No. 50-FZ);

Federal Law of April 7, 2020 No. 115-FZ "On Amendments to Certain Legislative Acts of the Russian Federation in terms of unifying the content of annual reports of state corporations, public companies, as well as in establishing the specifics of regulating corporate relations in 2020" (hereinafter — the Law of April 7, 2020 No. 115-FZ). Some of the provisions of this law were clarified by the letter of the Bank of Russia of April 9, 2020 No. IN-06-28 / 54 "On holding annual general meetings and distribution of profits in 2020";

Federal Law of July 31, 2020 No. 297-FZ "On Amendments to Certain Legislative Acts Regarding the Unification of the Content of Annual Reports of State Corporations, Public Companies, as well as Establishing the Specifics of Regulation of Corporate Relations in 2020".

The technical side of these decisions in some cases left much to be desired,[56] but in fairness it is necessary to take into account the extraordinary nature of these legal decisions caused by extraordinary circumstances, as well as the need to adopt new regulation in a short time.

The main provisions of the proposed measures were to change the timing of annual general meetings of shareholders in 2020 and remove restrictions on all decisions by annual general meetings in absentia (Articles 11 and 12 of the Law of April 7, 2020 No. 115-FZ).

It is noteworthy that none of these laws attempted to stimulate the use of electronic remote forms of interaction between participants in corporate relations (a shareholder and a joint-stock company, members of collegial management bodies) to overcome emergencies and / or create a new one, and / or improve current regulation. However, the objective circumstances that have developed in the context of the spread of COVID-19 and restrictive measures aimed at preventing its spread have led to a multiple

---

http://www.cbr.ru/collection/collection/file/31741/review_corp_14122020.pdf (accessed: 7.02.2021)

[56] For example, if Art. 2 of the Law of March 18, 2020 No. 50-FZ established a general rule that a meeting of shareholders, the agenda of which includes the issues specified in paragraph 2 of Art. 50 of the Law on Joint Stock Companies, in 2020, by decision of the board of directors of a joint stock company could be held in the form of absentee voting, then Art. 11 of the Law of April 7, 2020 No. 115-FZ has already suspended until December 31, 2020 inclusively, the effect of this provision.

increase in the use of remote electronic forms of interaction during general meetings of shareholders in 2020.[57]

It is quite obvious that the wide experience of using remote electronic interaction received by joint-stock companies and their shareholders in 2020 (we do not exclude that restrictions will remain in 2021) will never return the previous idea of corporate actions as meetings held by a groupof people gathering in one place and at the same time, and using the raising of their hands for the expression of their will. And the point is not only that this allows corporate actions to be carried out in a difficult epidemiological situation, the point is different: the modern development of technologies has led to what — remote electronic — interaction is — it is convenient for participants in corporate relations and much less costly for them.

Electronic technology, remote meeting participation, fully virtual meetings are the future of corporate action. Therefore, it is advisable to look at the essence of electronic and remote forms of interaction, at what legislative initiatives exist today in this area and at how we could institutionalize these forms in our legislation.

4. On electronic and remote forms of interaction in essence and on the prospects for the development of these forms in corporate law

An analysis of the specialized literature provides a basis for the conclusion that the use of electronic and remote technologies in corporate governance is partly a consequence of the evolution of electoral technologies. V. Fedorov notes that "the study of the world experience in voting automation makes it possible to identify similar and special characteristics of electoral devices, different principles of their operation, which indicate the existence of three large projects for the automation of voting and vote counting: mechanical (IV century BC — 1960-e years); electronic stationary (1860s — present); electronic distance (1996 — present)" [Fedorov V.I., 2020: 40].

[57] There is no complete statistics on this issue, however, it is the multiplicity of growth that is shown by the data provided in the publicly available information materials of the Central Securities Depository — the presentation "Service of electronic voting e-voting: advantages of use in new conditions", made on December 22, 2020.Available at: https://www.nsd.ru/upload/docs/conf/2020-12-22/preim.pdf(accessed 7.02.2021); available at: https://www.nsd.ru/publications/meropriyatiya/vebinary/vebinar-dlya-klientov-nrd-servis-elektronnogo-golosovaniya-e-voting-v-novykh-usloviyakh-itogi-goda-i/ (accessed: 7.02.2021)

In part, the use of electronic technologies for interaction between shareholders and joint-stock companies in Russian legislation, as noted above, is also following the examples of Western legal regulation (Directive 2007/36 / EU; Directive (EU) 2017/828).

If we analyze the issue of electoral electronic technologies, it will be obvious that one cannot equate the concept of "remote" voting and "electronic" voting. Electronic voting can be carried out at the place of the elections, but using special technical devices. Remote voting, on the other hand, is the vote of a person who is not present at the polling station. It can be assumed that such a distinction should be at the heart of modern legal decisions when changing the legislation on elections in Russia.[58] However, legal decisions regarding remote electronic voting cannot be called finalized yet, suffice to say that there are, for example, several definitions of the electronic voting in relevant legal acts.[59]

It is obvious that further development will follow the path of using remote electronic voting, which is clearly indicated by the Main Directions of Development of the Russian State Automated System "Elections" (Выборы) until 2022. One of the tasks that must be implemented by 2022, this document refers to the creation of a digital platform, on the basis of which the technical possibility of conducting remote electronic voting us-

[58] The Federal Law of June 12, 2002 No. 67-FZ "On Basic Guarantees of Electoral Rights of Citizens of the Russian Federation" provides a separate definition (Art. 2) for "electronic voting" (as voting without using a paper ballot, but with using technical means) and for "remote electronic voting" (voting without using a paper ballot but using special software".

[59] One of the definitions is given in the Federal Law of June 12, 2002 No. 67-FZ "On the Basic Guarantees of the Electoral Rights of Citizens" (Article 2), the other — in the Federal Law of May 23, 2020 No. 152-FZ " On conducting an experiment on the organization and implementation of remote electronic voting in the city of Moscow "; there are also relevant definitions in individual resolutions of the CEC of Russia in 2014 (for example, see: The procedure for remote electronic voting in the by-elections of deputies of the State Duma of the Russian Federation of the seventh convocation in single-mandate constituencies on September 13, 2020", approved by the CEC resolution of 27 July 2020 No. 261 / 1924-7 (para 1.2). In terms of content, they are similar, but there are some differences.

It is curious to note that similar processes are going on in relation to legislation on science in terms of holding meetings of dissertation councils, although they use their own terminology — "remote interactive mode ... subject to audiovisual contact with meeting participants" (see: Resolution of the Government of the Russian Federation of May 26, 2020 No. 751 "On the specifics of holding meetings of councils for the defense of dissertations for a scientific degree during the period of measures aimed at preventing the spread of a new coronavirus infection in the Russian Federation" (expires on August 1, 2021); Resolution of the Government of the Russian Federation of 20 March 2021 No. 426 "On Amending Certain Acts of the Government and invalidating Resolution No. 751 of May 26, 2020).

ing a personal account is implemented (with the user's identification on the ESIA — Unified identification and authentication system).[60]

Nevertheless, the state retains the possibility of another version of electronic voting — using special technical devices at polling stations (researchers talk about different options, for example, the technology of using complexes for processing ballots).[61]

Strictly speaking, the development of legislation on electronic and remote forms of interaction between participants in corporate relations could go hand in hand with the development of electronic stationary and remote electronic technologies in elections and during meetings of dissertation councils. However, as we saw from the description given above, there is no such correlation.

We see a clear trend towards increased use of electronic interaction, which was set in the framework of electoral and science legislation, but we do not see similar patterns. There is a difference in terminology, in addition, as already noted, the legislation on joint stock companies completely ignores the issue of using electronic devices when voting at a meeting of shareholders in person. The main emphasis was initially placed on electronic remote forms of interaction. The Bank of Russia in one of its materials, "Report on the assessment of the actual impact of the implemented proposals. Corporate Governance "(2016)[62] — very clearly described the needs for the implementation of the proposal to introduce electronic voting: providing the possibility of remote voting; optimization of operating costs for organizing the voting process; increasing the transparency of the voting mechanism; additional protection against fraudulent voting.

In another document — "Report for public consultations. On approaches to stimulating the activity of shareholders and investors to participate in the management of Russian public joint-stock companies "(2017),[63] the Bank made it very clear that increased attention to remote forms of inter-

[60] Federal State Information System "Unified system of identification and authentication in the infrastructure of state and municipal services in electronic form."

[61] See, for example: Resolution of the Central Election Commission of the Russian Federation of January 17, 2018 No. 129 / 1072-7 "On the use of technical means of counting votes — complexes for processing ballots during voting in the elections of the President of the Russian Federation" // SPS Consultent Plus.

[62] Available at: http://www.cbr.ru/content/document/file/84700/ofv_corp_gov.pdf (accessed: 9.02.2021)

[63] Available at: http://www.cbr.ru/content/document/file/50695/consultation_paper_170925.pdf (accessed: 9.02.2021)

action was caused by the need to increase the involvement of shareholders in the management of society.[64]

At the same time, it should be noted that the legislator still treats innovations in the regulation of electronic forms of corporate interaction with extreme caution — suffice it to say that all the are reduced to the regulation of hybrid meetings, when electronic forms of voting established by law (sending a message by e-mail; giving instructions through a nominee in electronic form; filling out a ballot on the website) are only additional opportunities for holding a meeting in person or absentee voting. Purely virtual or digital meetings — when all their participants interact electronically and remotely, the law does not provide.

From our point of view, the time has come to revise the current legislation in order to systematically describe the issues of electronic (including remote) interaction of participants in corporate relations.

There are now several initiatives in this area.

First, the draft amendments to the Federal Law "On Joint Stock Companies" in terms of creating the possibility of holding general meetings of shareholders in the form of a meeting by means of joint remote presence to discuss agenda items and make decisions on issues put to a vote, using information and communication technologies without specifying the venue "(project ID 02/04/09-20/00107789).[65] This draft proposes that in addition to a meeting in the form of joint presence of shareholders at the place of

[64] "It should be noted that in addition to special rules of law and 'soft regulation' aimed at stimulating the participation of shareholders in the management of the company, the company itself and its board of directors also have certain resources to increase the involvement of shareholders in the management of the company and must use them. The correct policy of interaction and effective channels of communication with shareholders can have a significant impact on the level of participation of minority shareholders in general meetings and their adoption of truly balanced decisions that meet the interests of both the shareholders themselves and the society as a whole. To do this, the company needs not only to simplify as much as possible the access of shareholders to the information on the basis of which decisions are made, and to make the process of participation in the general meeting as comfortable as possible for minority shareholders, for example, through the widespread use of modern information technologies, but also to create in shareholders a sense importance of their participation through the understanding that their opinion is taken into account by society when solving key problems and that they really influence the decision-making process in society and participate in its governance. A further consistent reduction in the costs associated with investor access to services that make it easier for investors to participate in the management of joint stock companies, in particular, a decrease in the cost of electronic voting on general meeting of shareholders, could potentially have a positive impact on the level of activity of Russian shareholders."

[65] Available at: https://regulation.gov.ru/projects#npa=107789 (accessed: 9.02.2021)

the meeting, a form of "joint remote presence" is also introduced; however, various hybrid forms of e-remote participation also remain permissible.

Secondly, the draft amendments to the Federal Law "On Joint Stock Companies" and certain legislative acts of the Russian Federation", introduced by the Deputy of the State Duma V.M. Reznik.[66] This project is less radical than the first in terms of innovations. The main innovation is the introduction of the concept of a "general meeting of shareholders with remote participation" ("a general meeting of shareholders of a company in the form of a meeting can be held using information technologies that make it possible to remotely participate in it, discuss agenda items and make decisions on issues put to a vote"). A distinctive feature of this project is the introduction of a special article for such meetings — "Features of preparation, convocation and holding a meeting with remote participation."

From our point of view, both legislative initiatives, despite some of their advantages, cannot be called optimal.

First of all, it should be noted that the proposed approach, when only the legislation on joint stock companies is changed, is incorrect. The problem of remote electronic participation in meetings is a problem for all legislation on legal entities, and not only corporate, but also unitary (there are also examples of the participation of several founders, as well as collegial bodies), and if you look more broadly,this is a problem that is relevant for all private legal entities. Accordingly, the changes should be of a systemic nature, which implies, first of all, a change in the provisions of the Civil Code of the Russian Federation both in terms of legal entities and in terms of civil law societies. Otherwise, we will receive non-systemic changes. And the risks are obvious here:

one part of the corporate legislation (legislation on business companies) will be changed, and the other part — in relation to business partnerships, farms — legal entities, cooperatives, non-profit organizations — will remain unchanged, and the participants of such corporations will be deprived of the opportunity to use information technologies in their activities;

there will be unreasonable differences in terms of the concepts used and legal means. And the risks of this are already visible. So, in 2020, the Government of the Russian Federation was instructed (following the meeting of the Council for the Development of Local Self-Government on January 30, 2020),[67] to amend legislation in order to provide an opportunity for

[66] Available at: https://sozd.duma.gov.ru/bill/1059849-7 (accessed: 9.02.2021)

[67] Available at: http://www.kremlin.ru/acts/assignments/orders/62919 (accessed: 11.02.2021)

citizens to send proposals on the agenda of the general meeting of homeowners in electronic form, and voting on these issues using a single digital platform.

This instruction was implemented by the adoption of the Decree of the Government of the Russian Federation of January 16, 2021 No. 9. This normative act established the possibility of voting in absentia by owners of premises in an apartment building using the "Single portal of state and municipal services". The possibility of using such a platform is, of course, a positive legal decision. However, the question arises: why is this opportunity offered only to residents of apartment buildings, and not to members of any corporations? It turns out that the owners of premises in apartment buildings will have the possibility of electronic remote voting using such a platform, and the participants of joint-stock companies will be deprived of such an opportunity, and for them the above draft laws imply other legal solutions. Interestingly, in the same year 2020, an instruction of a more general nature was issued — Pr-1726GS, clause 8b) (from the List of instructions following an expanded meeting of the State Council Presidium, held on September 28, 2020).[68]

In accordance with this instruction, the Government of the Russian Federation should create conditions for the transition mainly to document automation in the interaction of citizens registered on the specified portal, organizations and authorities, providing for the possibility of integrating with this platform the electronic document management systems of public authorities of the regions of the Russian Federation, local governments and organizations. In fact, the nature of the order makes it possible to form a single platform for voting by members of various corporations and civil law companies.

It is quite obvious that various political and legal impulses should be at least correlated with each other for the purpose of creating general conditions for remote electronic interaction of participants of various legal entities and civil law communities. The specific changes that are currently proposed by these projects (apparently, there will be other initiatives) will only lead to confusion in the legislation, the "ragged" nature of its changes, the designation of the same institutions by different terms.

In general, it seems to us idea of correlation between private law and public law regulation of electronic interaction is very rational. Of course,

[68] Available at: http://www.kremlin.ru/acts/assignments/orders/64273 (accessed: 11.02.2021)

specifics of the electoral process and the defense of dissertations will remain, but the basis for such interaction will be common, the terminology will be unified; perhaps we will even have common services (you can also call them the buzzword "platforms") for such remote electronic interaction, which will undoubtedly facilitate the tasks of its participants. To implement this idea, however, a certain conceptual basis is needed, as well as a serious interdisciplinary scientific and expert study of the issue.

With regard to changes in corporate legislation in general and legislation on joint stock companies in particular, from our point of view, the most optimal approach would be the following:

making general changes to the Civil Code, which allow the use of electronic forms of interaction between participants (founders) of legal entities, as well as in the activities of any civil law communities; it is also necessary to secure the possibility of such interaction with other participants in corporate procedures (creditors, first of all), as has already been done in separate laws. Then a general draft law should be prepared, which would introduce systemic changes to individual laws, synchronized in the general logic;

Civil Code and other special laws should assume the possibility of:

information electronic exchange on various grounds (notification of a meeting (meeting), information on the issues under consideration by electronic means, etc.);

use:

virtual meetings; here, the concept of "joint remote presence" proposed by one of the indicated projects is quite suitable, although variants are also possible; at the same time, such a decision requires careful regulation, and, possibly, at the first stage, special regulation by bylaws, including in the form of a legal experiment;

various types of voting at hybrid (mixted) meetings, when some of the participants are present in person, including remotely (online), and some participate in absentia (including using electronic interaction): electronic stationary voting; remote presence (participation and voting); remote electronic absentee voting;

the holding of hybrid meetings should be regulated in detail in each special law that will provide for it; at the same time, the possibility of using electronic stationary voting may be provided for use by the charter of any legal entity with a description of how specifically (with the use of what

technical means) it is carried out; specific civil law communities will also require special regulation;

remote electronic absentee voting can be carried out during hybrid (mixed) meetings;

in the form of filling out electronic bulletins on specialized electronic resources (platforms);

in the form of sending the voting results by e-mail;

in the form of voting through the intermediary system (what is called the e-proxy voting mechanism);

for various legal entities, differentiated rules for remote electronic absentee voting may be provided — it is obvious that the last option — by the e-proxy voting mechanism — is, rather, for joint stock companies in which there is a system of intermediaries — nominee holders. Such a complex model implies the need for a special description of the procedure for registering and accounting for votes, which, again, will differ for different types and types of legal entities;

public joint stock companies must by law (and not simply because of such a possibility in the charter) provide the possibility of holding both fully virtual meetings and mixed (hybrid) meetings of shareholders. At the same time, the Law on Joint Stock Companies requires a complete revision of that part of it that regulates the preparation and conduct of meetings, with the aim of systematically describing both traditional meetings, mixed (hybrid) meetings, and virtual meetings. The method of making point changes, which is currently used, should be excluded, it leads to an unjustified complication of the normative material;

separate regulation requires the implementation of electronic forms of interaction for those shareholders who own shares of the joint-stock company in the form of digital financial assets, the release of which (digital financial assets certifying the rights to participate in the capital of the joint-stock company) became possible after the adoption of the Federal Law of July 31, 2020 No. No. 259-FZ "On digital financial assets and digital currency" (Art. 13).

References

Alekseev R.A., Abramov A.V. (2020) Issues and prospects of using electronic voting and electoral blockchain technology in Russia and abroad. *Grazhdanin*. *Vybory. Vlast*, no 1, pp. 9–21 (in Russian)

Antonov Ya.V. (2015) Development of legal regulation of electronic voting in Russia. *Upravlenchekoye consultirovanie*, no 5, pp. 63–71 (in Russian)

Bataeva B.S. (2020) Development of corporate governance using electronic voting services. *Upravlencheskie nauki*, no 2, pp. 74–87 (in Russian)

Chekhovskaya S.A. (2016) Modern development of corporate legislation. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 2, pp. 74–86 (in Russian)

Chekhovskaya S.A. (2018) New contours of corporate law. *Predprinimatelskoye pravo*, no 3, pp. 31–41 (in Russian)

Druzhinin A. (2012) What is the most effective way to use electronic means of communication during GMS? *Aktsionernyi vestnik,* no 9, pp. 38–44 (in Russian)

Elnikova E.V. (2020) The use of digital technologies in voting at the general meeting of participants (shareholders) of a business company. *Vestnik universita imeni O.E. Kutafina,* no 7, pp. 60–67 (in Russian)

Fedorov V.I. (2017) Electronic voting: a fix idea or the foundation of future democracies? *Grazhdanin. Vuboru. Vlast*, no 1–2, pp. 170–185 (in Russian) Fedorov V.I. (2020) Projects of automation voting in a historical retrospective. *Grazhdanin. Vuboru. Vlast*, no 1, pp. 34–55 (in Russian)

Gabov A.V. (2020) Force majeure, coronavirus and decisions of authorities aimed at preventing its spread. *Zakon,* no 5, pp. 152–171 (in Russian)

Gontar S.G. (2019) Electronic voting — a new opportunity for citizens to participate in the formation of government bodies. *Gosudarstvennaya vlast and mestnoye samoupravlenie*, no 4, pp. 29–33 (in Russian)

Grigoriev A.V. (2020) Constitutional regulation of the use of modern information and communication technologies in the implementation of direct democracy institutions in Russia. Candidate of Juridical Sciences Summary. Moscow, 30 p. (in Russian)

Kersting N. (2007) Electronic voting and democracy in Europe. *Politicheskaya nauka,* no 4, pp. 123–144 (in Russian)

Khamutovskaya S. (2019) New voting technologies: foreign experience. *Nauka i innovatsii*, no 4, pp. 39–42 (in Russian)

Kolyushin E.I. (2020) Legal issues of remote electronic voting of voters. *Constitutionnoye i municipalnoye pravo*, no 2, pp. 25–30 (in Russian)

Kraakman R., Apmour J., Davies P., Enriques L., Hansmann H., Hertig G., Hopt K., Kanda H., Pargendler M., Ringe W.-G., Rock E. (2017) *The Anatomy of Corporate Law.* 3rd Edition. Oxford: University Press, 281 p.

Lanskov D.P., Danilova S.A. (2019) Complex of electronic relations between registrars, issuers and shareholders. *Aktsionernoye obschestvo: voprosy corporativnigo upravlenia*, special issue, no 9, pp. 13–17 (in Russian)

Lysenko K.V. (2019) The choice is everything! *Aktsionernoye obshestvo: voprosy korporativnogo upravlenia,* no 9. Available at: URL: https://ao-journal.ru/journal/lib/ejournal/detail/ArticleID/1711/vybor-reshaet-vse (accessed: 4.02.2021) (in Russian)

Magdalinskaya Yu.V. (2020) Peculiarities of legal regulation of electronic voting of shareholders (e-voting). *Informationnoye pravo*, no 1, pp. 44–48 (in Russian)

Matrenina K.Yu. (2017) Formation of electronic voting at elections in the Russian Federation and the prospects for its development (constitutional-legal study). Candidate of Juridical Sciences Thesis. Tyumen, 224 p. (in Russian)

Medvedeva T.M., Azimova L.V. (2020) Electronic technologies in corporate relations. *Khozyaistvo i pravo,* no 9, pp. 65–79 (in Russian)

Murashov M.V., Papin E.N., Voziyan V.Yu. (2020) Electronic voting — a new level. *Aktcionernoye obschestvo: voprosy corporativnogo upravlenia,* no 9. Available at: URL: https://ao-journal.ru/) (accessed: 10.04.2021) (in Russian)

Novoselova L., Medvedeva T. (2017) Blockchain for shareholders voting. *Khozyaistvo i pravo,* no 10, pp. 10–21 (in Russian)

Pavlushkin A.V., Postnikov A.E. (2009) Legal mechanism of remote electronic voting (analysis of a possible model). *Zhurnal rossiyskogo prava*, no 11, pp. 5–13 (in Russian)

Saccone F. (2010) E-Proxy reform, activism, and decline in retail shareholder voting. The Conference Board Director Notes no DN-021. Available at: https://ssrn.com/abstract=1731362 (accessed: 1.03.2021)

Sychev P.G. (2011) New legislative initiatives: protection of the corporate governance system or a gift to raiders? *Bezopasnost biznesa*, no 1, pp. 30–34 (in Russian)

Tsaplin A.Yu. (2016) Prospects for remote electronic voting in Russia. *Izvestia Saratovskogo gosudarstvennogo universiteta. New Seria: Sociologia. Politologia*, no 3, pp. 345–350 (in Russian)

Zakuskin A.A. (2019) Introduction of electronic technologies into the Russian electoral process. *Vestnik Mariyskogo gosudarstvennogo universiteta. Seria Istoricheskie nauki*. *Yuridicheskie nauki*, no 3, pp. 277–281 (in Russian)

Zetzsche D. (2007) Virtual shareholder meetings and the European shareholder rights directive: challenges and opportunities. Available at: https://ssrn.com/abstract=996434 (accessed: 1.03.2021)

Zhiznenko O. (2020) How electronic voting of shareholders is developing in Russia and the world. Available at: URL: https://pro.rbc.ru/demo/5e2aa3819a794768c792e071 (accessed: 4.02. 2021) (in Russian)

Smart contract: from definition to certainty

Yuriy Truntsevsky

Professor, Leading Researcher, Department of the Methodology of Counteracting Corruption, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Doctor of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya St., Moscow 117218, Russian Federation. E-mail: trunzev@yandex.ru

Vyacheslav Sevalnev

Candidate of Juridical Sciences, Institute of Legislation and Comparative Law under the Government of the Russian Federation. Address: 34 Bolshaya Cheremushkinskaya St., Moscow 117218, Russian Federation. E-mail: sevalnev77@gmail.com

Abstract

The purpose of the present article is to gain an understanding of the opportunities and difficulties created by the introduction and development of the practice of network (smart) contracts. Our research methodology is based on a holistic set of principles and methods of scholarly analysis employed by modern legal science. It uses a dialectical method involving both general approaches (structural system method, formal logical method, analysis and synthesis of individual elements, individual features of concepts, abstraction, generalization, etc.) and particular methods (legal technical, systematic, comparative, historical, and grammatical methods, method of the unity of theory and practice, etc.). We analyze the views of lawyers and other specialists from Russia and abroad, legislative innovations in the field of digital technologies, the practice of blockchain-based smart contracts, and the main risks (whether legal, technological, operational, or criminogenic) of smart contracts for economic activities with a study of their causes. In the present-day situation, it is necessary to move from the legal definition of the smart contract and its legal and technological characteristics, advantages and disadvantages to the implementation of startups in a wide range of areas, especially business, public regulation, and social relations. Scholarly and information support for such processes will contribute to the development of industry, public administration and digital technology applications to improve the life of individual citizens and society as a whole. The introduction of smart contracts does not require the adoption of new laws or regulations. Instead, one should adapt and, possibly, modify existing legal principles at the legislative and judicial levels to pave the way for the use of smart contracts and other new technologies. The system of contract law provides a sufficient framework for regulating transactions without the introduction of any new legal categories. We propose approaches to the legal definition of the smart contract and identify a set of problems that must be solved at the legislative and technical legal levels in order to implement smart contracts effectively in different spheres of life.

Keywords

smart contract, blockchain, technology, contract law, risk, Internet of things, court.

Acknowledgments: The paper was written with support of the Russian Foundation for Basic Research (project no 18-29-16023).

For citation: Truntsevskyi Ju.V., Sevalnev V.V. (2021) Smart contract: from definition to certainty. *Legal Issues in the Digital Age,* no 1, pp. 100–122.

DOI: 10.17323/2713-2749.2021.1.100.122

Introduction

Network, or smart contracts (SC) have been attracting the keen interest of legal scholars and lawyers on account of their potential impact on contractual relations. The basic research problem in this domain is to study past practice and analyze obstacles to the introduction and improvement of SCs in Russia and other countries as well as to predict their future development and new spheres of application in the context of the exponential growth of digital technologies [Khabrieva T.Y., 2018: 5–16]; [Khabrieva T.Y., Chernogor N. N., 2018: 85–102].

SCs are indeed a revolutionary instrument. They can be used to decentralize many processes that people employ today and to improve existing solutions in a radical fashion. For example, E. Hughes[1] has said that these technologies shall be brought by people who are sick and tired of government corruption and aggressive politics. At the same time, blockchains are still fraught with legal difficulties, and the law makes no mention of contracts based on this technology. There is a clear need to make a legal definition of this phenomenon.

In recent years, blockchains have fostered the emergence of SCs, which are being used at an ever greater rate [Perov V.A., 2017]; [Ivanov A.Y., 2017]. Speaking at the We Are Developers World Congress 2018 in Vienna, Apple co-founder S. Wozniak said that blockchains shall have an immense impact on the technology sector, calling them the "next major IT revolution that is about to happen."[2] Programmers and lawyers should

[1] A US mathematician and programmer, one of the founders of the cyberpunk movement.

[2] Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-steve-wozniak-blockchain-apple-cryptocurrency-revolution-a8357336.html (accessed: 2.08. 2019)

cooperate on SC development. One needs dictionaries that connect legal language and computer code. Scholars must pool their efforts to develop technically advanced applications and powerful analytic tools.

SCs are attracting the keen interest of different industries due to their possible use in performing and automating certain actions in order to save time and money. There can be a lot of commercial benefit from using SCs for automatically calculating the payments due and the goods to be delivered by each party.

Possible domains for automating legal processes include operations such as due diligence, searching for clients, round-the-clock emailing and notification, document processing, model agreements, and other processes involving a high degree of regulation.

The introduction of SCs will lead to reduced paperwork and smaller, more frequent payments, improving cashflow while reducing potential problems thanks to more precise tracking and verification of the performance of contractual obligations. It will reduce human involvement and assure the total transparency of responsibilities and financial matters, making all economic sectors more accountable, transparent, effective and productive. "Smart documents" will make it possible to draft high-quality documents faster and more precisely, allowing lawyers to focus on fine details and negotiations between parties [Golovanova A.A. et al., 2019: 212]. Over the next five or ten years, "traditional" legal work should become increasingly automated [Anisimov V.F., Sergevnin V.A., 2018: 11–16].

The use of SCs poses interesting new questions in the domains of law and technology. Besides legal issues relating to the creation and use of SCs, there also exists the problem of their enforcement. In particular, one must determine which types of conflict resolution mechanisms can be used (or have to be created) and which types of legal remedies are or should be available in view of the immutable nature of the blockchain technology on which SCs are based.

Nevertheless, even if SCs are not legal contracts per se, they "are not in a legal vacuum," as Meyer and Eckert[3] put it [Chandler S., 2019]. Even if the terms governing the relations between parties are not governed by law, SCs will still fall under national law or international agreements if they lead to such violations as drug trafficking. At the same time, SCs are associated

[3] Stephan Meyer and Martin Eckert are blockchain legal experts at the MME law firm in Zurich and Zug. Available at: https://finance.yahoo.com/news/smart-contracts-no-problem-world- 123200100.html (accessed: 2.08.2019)

with a high level of legal risks that must be meticulously reduced in order to assure effective legal products and services.

Given the intersectoral and multidimensional nature of our subject, we conducted a comprehensive study of the following aspects of the problem:

Analyzing conceptual approaches to the legal regulation of FinTech and RegTech in Russia and abroad with regard to SCs;

Comparing the theoretical foundations, technical possibilities, and practical level of introduction and legal support of SCs;

Making a comparative legal analysis of the legal framework of SCs;

Analyzing the potential impact of digital technologies on law and society and on legislative activities aimed at reforming the economy and identifying economic sectors that require the introduction of SCs.

1. Current Research

SCs have received increasing attention in recent years due to their growing use, the adoption of official documents in the digital economy sphere, and the introduction of legal regulations. A search with the keyword "smart contract" on e-library.ru produced the following results (as of August 10, 2019):

This phrase figures in the titles of 152 publications, including 74 journal articles, 32 books, 65 conference proceedings, 2 reports, 2 patents, and 0 dissertations.

The number of publications with the phrase "smart contract" in their titles has the following chronology: 0 publications in 2016, 13 in 2017, 100 in 2018, and 39 during the first six months of 2019.

The phrase "smart contract" occurs 465 times in titles, abstracts and keywords (2 in 2016, 52 in 2017, 308 in 2018, and 103 during the first six months of 2019).

The content analysis of the use of the phrase "smart contract" shows that the first publications to mention SCs in Russia were papers by E. Popova, N. Popov and A. Zemtsov [Zemtsov A.N., 2016: 24–26]. In the citation impact, the articles by A. Savelyev [Savelyev A. I., 2017: 94–117] and E. Popova and N. Popov [Popova E.M., Popov N.V., 2016: 9–14] have been the most cited. Of the 20 publications with the greatest citation impact, 10 were devoted to legal matters, and the rest to technical, economic and managerial issues.

Some scholars have conducted a legal analysis of SCs in the narrow sense, focusing on "the use of computer code for generating, verifying and executing agreements between parties"; the key legal issues here were notification, consent and protection of consumer rights' [Efimova L.G., Sizemova O. B., 2019: 23–30]; [Dolova M.O., 2019: 27–36]. Other authors have studied the problem from the standpoint of traditional civil law without isolating SCs from legal institutes [Kamalyan V.M., 2019: 20–27]; [Kalinina A.L., 2019: 37–45]; [Nagrodskaya V. B., 2019: 128]. Another group of scholars has written about the dual legal nature of SCs: they are technological solutions with a computer protocol that are not agreements, on the one hand, and agreements between parties in electronic form that have legal force, on the other [Shaidullina V.K., 2019: 21–23]. Finally, some practical specialists have examine possible conflict between SCs and theory of relational contracts [Gromova E. A., 2018: 34–37].

Many authors essentially recognize the fact that an SC is a type of computer code that can represent all, a few or one of the existing forms of contracts recognized by law [Nosov S. I., 2019: 6–13]; [Makarchuk N. V., 2019: 40–43]. Thus, even when the SC wholly refers to a legally binding agreement (often called a "smart legal contract"), it is still governed by contract law just as any agreement written in natural language.

As a result, most scholars believe that traditional contract law will continue to function in the age of SCs, and that the latter "will never fully replace the law of natural language." Nevertheless, they say that SCs may help to increase the clarity, predictability, verifiability and ease of enforcement of contractual relations. Unfortunately, no comprehensive scholarly study of the legal consequences of such contractual practices has appeared so far.

After collecting basic information about this new phenomenon, the aforementioned studies try to identify the areas in which these contracts differ from traditional contracts, examine whether SCs can be inscribed into the existing national legal framework, and recommend changes in contract law that would simplify their use and assure their legal effectiveness. They also attempt to answer such topical questions as "are SCs legally binding agreements?" and "will they replace traditional contracts?"

Studies of the legal problems connected with the introduction and use of SCs examine three different stages: contract generation and improvement; execution and modification; and violations and legal remedies thereto.

Foreign legal scholars have not been able to reach a consensus on the definition of SC, proposing many different approaches [Stark J., 2016].

This is not surprising given the nature of this new phenomenon and the complex technologies on which it is based. The simplest definition used in scholarly discussions is that the SC is an agreement between two or more parties that is coded in such a way that its correct implementation is guaranteed by a blockchain [Wattenhofer R., 2016]. Note that such a definition involves not only a digital contract between parties written in computer code but also a decentralized ledger (blockchain). This explains why a blockchain such as Ethereum is usually employed as the decentralized execution platforms that stores the SC [Bashir I., 2013].

At the same time, the SC has no need of a blockchain to function: no one can prevent the creation of SCs that are embedded into a traditional database. However, in this case, the parties would have to rely on a trustworthy centralized party, and the ledger would not be as immutable as in the case of a blockchain. As a result, such a contract would no longer be "smart," although it would be effective on account of the security that it provides thanks to its immutability and digital distribution among users.

As a rule, such legal studies end with the constatation that the SC conforms to the principles of contract law. Authors propose different legal remedies that can be applied to SCs and urge legislators and lawyers not to ignore their utility for assuring legal security.

2. Legal regulation of the application of smart contracts

The term "smart contract" does not figure in Russian legislative acts. Some normative legal acts have begun to mention this notion in recent years, however. For example, Order of the Russian Government no 2101-r "On approving a comprehensive plan for modernizing and expanding the trunk infrastructure up to the year 2024" of September 30, 2018,[4] mentions that "the main cross-cutting data processing technologies in the transport industry that are planned for introduction during the implementation of the transport section of the plan include technologies of self-executing codes for performing obligations ('smart contracts')." Alongside the sections "Public report: national assessment of the risks of legalizing (laundering) criminal income. Main conclusions for 2017–2018" and "National assessment of the risks of financing terrorism: public report for 2017–2018,"[5] Memorandum

[4] Sobraniye Zakonodatel'stva Rossiyskoy Federatsii. 2018. 42(II), §6480 // SPS Consultant Plus.

[5] Vestnik Banka Rossii. 2018, August 29.

of the Bank of Russia IN-014-12/54 "On the national assessment of the risks of money laundering and financing terrorism" of August 14, 2018 includes the section "Transferring capital with the help of unregulated entities" whose item "Measures taken in the Russian Federation for managing risks" notes that "work is being conducted for making changes to Russian law so as to define and determine the status of digital technologies used in the financial sphere (including 'distributed ledger technology,' 'electronic letter of credit,' 'digital mortgage,' 'cryptocurrency,' 'token,' and 'smart contract')…"

The State Duma has adopted the laws "On amendments to the first, second and fourth parts of the Civil Code of the Russian Federation"[6] and "On attracting investments with the help of investment platforms and amending certain legislative acts of the Russian Federation,"[7] which will enter into force on October 1, 2021; as a result, section 160, item 1, of the Russian Civil Code will define the SC as "an agreement employing electronic or other technical means" and relating to an agreement in written form. These regulations shall serve as the foundations for drafting a new law on digital financial assets (cryptocurrency and tokens).[8]

It should be said that Russian legislators are still looking for ways of juridically defining the legal status of SCs in different areas of economic activity and public governance, among others. To cite L. Cheng, founder of smart contract service provider Vanbex, "The legal world has yet to fully assimilate the new realities of technology, including smart contracts. So ultimately the answer to this question will lie in the individual legal processes in jurisdictions around the world" [Chandler S., 2019].

With regard to foreign experience in the legal regulation of SCs, 47 US states adopted the Uniform Electronic Transactions Act (UETA) in 1999, setting down rules for electronic contracts, records and signatures and affirming the validity of electronic contracts and of the use of electronic signatures for expressing consent to an agreement. Nevertheless, in 2017 some states decided to adopt supplementary rules in view of the large-scale use of SCs. Arizona passed laws that allow securing SC signatures through the blockchain technology. Vermont and Nevada recognize blockchain-based contracts as acceptable evidence for conflict resolution. Delaware permits the registration of shares of Delaware companies in blockchain

[6] SPS Consultant Plus.

[7] SPS Consultant Plus.

[8] Federal bill 419059-7 "On digital financial assets" Adopted by the State Duma in first reading on May 22, 2018 // SPS Consultant Plus.

form. Section 5 "Blockchain Technology" of Arizona law HB 2417 defines a smart contract as "an event-driven program that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."

Western legal scholars [Gatteschi V. et al., 2018: 3] note that SCs have need of standardization: if different economic sectors continue to develop SCs in the absence of standards, companies will not derive full benefits from blockchain solutions. Such standards should assign responsibilities for SC development and operation and specify conflict resolution mechanisms, creating the presumption of the legal nature of SCs provided that they have certain properties and are used by market players in a certain way. This already exists in some domains: ISDA (International Swaps and Derivatives Association) provides master agreements for certain financial operations, while NVCA (National Venture Capital Association) is elaborating model legal documents for startups.

3. Legal description of smart contracts (definition)

Why are SCs "smart"? After all, they are neither artificial intelligence nor capable of machine learning. They only perform the actions they are instructed to perform.

Can they be called contracts? Courts have not ruled on this so far. Probably the answer to this question depends on the adoption of the "computer code is law" doctrine. Still, SCs — whether fully coded or in Ricardian form[9] — will most likely have to fulfill all the requirements of a legal contract to have legal force. A recent example of the use of SCs is Fizzy AXA.[10] AXA is the first major insurance company to offer insurance policies based on blockchain (100% automated, 100% safe platform of parametric insurance against flight delays): if a client's flight is more than two hours late, he or she automatically receives compensation for the delay; a delay of over two hours triggers the irrevocable action of transferring an automatic deposit that compensates for the client's losses.

[9] In 1996, Ian Grigg and Gary Howland defined the Ricardian contract as a bridge between a textual contract and computer code that has the following features: (a) a contract offered by an issuer to holders, (b) for a valuable right held by holders and managed by the issuer, (c) easily readable (like a contract on paper), (d) readable by programs (parsable like a database), (e) digitally signed, (f) carrying the keys and server information, and (g) allied with a unique and secure identifier [Grigg I., 2004: 25–32].

[10] Available at: https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy (accessed: 2.08. 2019)

Some foreign specialists [Navas Navarro S. et al., 2017] argue that SCs are neither ordinary contracts nor "smart" contracts and propose a different name — "program-executed transactions" — on the basis that they are not contracts but software. At the same time, the notion of "contract" is based on the desire of the parties to program its terms and values and, even more importantly, to create SCs as an alternative to traditional contracts.

Let us now take a closer look at SCs. There is a lot of rhetoric and propaganda about what they are or should be. Nevertheless, the reality is that SCs are software. They are coded in a state-of-the-art computer language such as Solidity. An SC is embedded in a blockchain and has access to its inner functions. At first sight, SCs may seem to be a clever idea that permits the infinite expansion of the basic technology of the "immutable distributed ledger" into which they are embedded and which considerably improves the flexibility of SCs and expands their areas of application.

A contract is typically an agreement between parties that must be executed by law. Contracts stipulate what each party must to do. Nevertheless, the development of the blockchain technology permits the automatic execution of contractual terms. This is made possible by the SC, which is a set of promises in code, including protocols through which the parties execute these promises.

Most legal contracts are based on templates that contain standardized legal formulations into which different terms can be inserted. These contracts mostly rely on third parties (courts, arbiters, guarantors, etc.) for their execution. This process is redundant and wastes a lot of time and money as well as being unpredictable. Yet all of this can be eliminated with the help of SCs that contain codes that can execute the terms of a contract automatically. The code of a contract defines its terms as a set of syllogisms in a similar way to a legal document.

Whereas an ordinary contract sets out the terms of mutual relations (that are legally binding, as a rule), a "smart" contract assures the respect of its terms with the help of cryptographic code. In other words, an SC is a program which, regardless of whether it is called a contract or not, allows the automatic execution of a contract that is either contained directly in the SC or associated with the SC, which serves as its compulsory execution mechanism coded in blockchain.

One typically cites the following characteristics of SCs [Savelyev A.I., 2016: 32]; [Ream J., 2016: 16]:

electronic nature;

software based on the "code is law" principle that will be created at the demand of the parties and subsequent subscribers.

Higher reliability (certainty and accuracy). Whereas an ordinary contract, whether oral or written, is interpreted by human beings, the SC consists of computer code that is interpreted by computers. These codes have the advantage of being precise, so that all parties can predict the outcome of the contract. Such a contract is verifiable insofar as it is coded in blockchain and so has only one copy, incontestable evidence of its existence, and settled terms.

Conditionality. Computer codes follow the logic "if this, then that." The parties set down their terms with the help of a conditional statement that assures the execution of the contract.

Autonomy and independence: after the SC is agreed upon and launched, the execution of its codes takes place automatically without any special approval mechanism. Thus, the parties to the contract (and even third parties) are unable to stop this process even if they have second thoughts or make programming errors. For example, if a money transfer is arranged (e.g., scheduled for the first Sunday of each month over the next five years), then the transfer will take place on this specific day and in the initially specified amount over the next five years. This feature leads to the greater certainty of SCs.

Speed. The processes of preparing contracts and auxiliary documents are automated with the help of computer code rather than being drafted by hand. In addition, updates can be made in real time.

Lower cost. Money is saved insofar as less time is needed to fill out contracts, smaller wages are paid to employees to carry out such tasks, and future costs are reduced due to fewer errors and especially fewer intermediaries for verifying and executing contracts.

Security. SCs and their data are stored in a decentralized register which is secured with the help of cryptography. They cannot be lost, as each party has a copy, and are extremely difficult to hack. Even if a hacker manages to penetrate into the blockchain with the help of arbitrary addresses, he will be unable to access personal information.

New businesses and operational models. Such SC characteristics as lower costs, etc., create new opportunities. For example, electric cars can be charged by induction while standing on streets or at traffic lights with the help of SCs.[11] The system known as the "Internet of Things" (IoT) connects

[11] The world's first electric road that charges moving electric cars opens near Stockholm. Available at: https://fishki.net/2570200-pervaja-v-mire-jelektrificirovannaja-doroga-dlja-zarjadki-jelektromobilej-otkrylasy-v-shvecii.html (accessed: 2.08. 2019)

computerized objects (for example, cars, kitchens, heart monitors, etc.) to the Internet in order to communicate data without any direct human involvement. The SC can execute its terms by interacting with digital objects.

SCs must be capable of automatically detecting events (if the event launches SC code and meets a pre-set criterion). For example, a rental car may be specially programmed to receive instructions connected to an SC and, if the debtor does not pay for the service, the car will not start [Tjong Tjin Tai E., 2017].

Can one amend SCs? This is a crucial question for the SC movement. The commonly held view is that there should be no return after the terms are set down in code, as automatic implementation and immutability are key features of SCs.

Nevertheless, this question should be answered for all types of SCs and especially for cases where SC execution can violate the law. Consider, say, an SC that specifies that the debtor must retain certain goods that could be confiscated by the creditor in 60 days. Some time later, the law is amended, and a new minimum delay of 120 days is set down. In this case, the contract was drafted correctly yet subsequently contradicted the law due to legislative changes. Would the SC continue to execute automatically, as initially agreed, and thus violate the law?

There are two possible ways of solving this problem: they may be called "public" and "private." In the first (*ex ante*[12]) approach, governmental agencies create a public database containing important regulations that can permit the SC to detect legal updates and update its terms. In the second (*ex post*[13]) approach, the state does not create such a database, letting the parties control the SC themselves. The disadvantage of such an approach is that parties can try to insist on the introduction of certain changes to further their own interests. To minimize this possibility, the contract should identify terms that can be changed (e.g., the fee) and the terms that cannot be changed under any circumstance (e.g., the contract deadline).

Thus, SCs are computer code that automatically executes terms set down by the parties for regulating their relations. The idea is to make the contract self-supporting, rendering its modification very complicated. If a conflict arises between the parties, the injured party will go to court only after the improper fulfillment or unjust enrichment, as the SC has already been or is being executed.

[12] Ex ante refers to the modelling of future economic phenomena and processes.

[13] Ex post refers to actual results attained by the economy over a certain period.

Although SCs are specially designed to avoid contract violations, they can be invalid if they lead to unlawful results, e.g., drug trafficking or selling alcohol to minors. The following actions may be taken to minimize these problems:

Writing computer codes in a precise manner and with variables that can be adapted to the law and its amendments. The parties should set down the terms in accordance with existing law and with the possibility of their future adaption to changes.

Explicitly prohibiting certain items in SCs (e.g., drugs), which requires (1) promulgating standards for the content of SCs (e.g., when selling expensive goods, a certain sum must be held on a special account to avoid violating tax rules, etc.), (2) embedding systems that detect violations of the law (e.g., when interest on a loan becomes usurious) or require identification to prove the lawfulness of a contract (e.g., the purchase of alcohol by minors).

Using not only SCs but also written contracts with an influence on the former for the purpose of minimizing discrepancies. In particular, people today still want to have contracts in hard-copy form that would be tangible and understandable to the average person. SCs could be used either to code terms that are not significant or exclusively to execute the terms of a written contract. In this case, one could adopt the proposal of the Russian Federal Tax Service to develop XML economic contracts.

If a textual version of the contract is also drafted.

The parties should discuss the possibility of distributing risks in the case of coding errors.

The textual agreement attached to the code should indicate the applicable law as well as determining the priorities of text and code in the event of a collision.

The textual agreement should include a statement by each party that it has seen the SC code and that the latter reflects the terms contained in the textual agreement.

The textual agreement can be submitted as evidence of the terms of the contract to a court.

When an ordinary contract is violated, the injured party brings an action to court for indemnity, specific execution or compensation for the inflicted damage.

Thus, the SC should lead to the appearance of a new type of lawyer who will be a specialist in both law and computer science. In practice, programmers and lawyers are already cooperating on the solution of legal and technical issues. When lawyers create SCs, a team of professionals in the fields of law and technologies has to work together. Nevertheless, there is still a lot of room for innovation in this domain.

4. Areas of application of smart contracts (certainty)

It is easy to imagine how SCs could be applied in different industries and operations from wholesale deliveries to leasing equipment.

A more complicated task is to create SCs that can be used by companies. A number of enterprises are working on SC templates that companies could adapt to their needs.[14] Slock is launching a program called "Alpha" that companies can use to integrate solutions for the sharing economy. Jincor is one of many enterprises working on templates that would meet legal norms and cryptocurrency standards. Companies can also hire programmers to create original SC solutions. This is a new domain, and so the offer is still quite limited. At the same time, companies must understand what processes they want to automate in their business with the help of SCs and calculate the savings that this automation would provide.

Thus, SCs have become a hot topic insofar as an ever greater number of applications are appearing in different industries (from the food industry and agriculture to financial services and insurance). SCs are attracting attention thanks to the opportunities they can provide: the distributed ledger technology should make SCs a better and more automated way of signing and executing contracts.

Although SCs are still relatively rare today, they can be used in virtually any scenario for transmitting and storing secure immutable data without intermediaries.

Here are a few examples.

Financing commerce. Today, commerce is often financed by banks for maintaining liquidity and raising trust in the exchange of assets. SCs can be used to facilitate the financing of commerce with the help of various data sets such as bills of lading, GPS and customs data. SCs can use such general control points for implementing full or partial payments, transferring

[14] Available at: https://www.reuters.com/brandfeatures/venture-capital/article?id=59712 (accessed: 2.08.2019)

property rights, and issuing reimbursements when the contractual terms are violated.

Healthcare. Public health computer systems store millions of medical records. Although healthcare organizations have invested enormous funds in security, current access and storage methods are a lot more vulnerable to cyberattack than their blockchain-based equivalents. Blockchain-based SCs can also be used to issue prescriptions, present bills, manage property, store test results, etc.

Medical studies. This industry produces important medical data, including test results and new drug formulas that must be kept secure and secret. They can be secured with the SC technology, which can also be used to communicate information to third parties for different reasons. This is only one example of how smart blockchain-based contracts can be beneficial for the medical research industry.

Property rights. SCs have two major areas of applications here. First of all, they can be used for registering property rights: the rapidity and low cost of SCs give them an advantage over existing systems in recording rights to all types of property from land and buildings to phones and watches. Secondly, the use of SCs on the real estate market can render the expensive services of lawyers and real estate agents superfluous. Instead, they will allow sellers to process transactions on their own.

Moreover, all intellectual property rights from royalties (from copyrights and trademarks, say) to patent licensing fees can be turned into SCs. Oracles can employ IP address databases for checking property rights and transferring payments from users to IP address owners. SCs can also be used to store information about the partial ownership of IPs and allocate the corresponding shares to persons.

Mortgages. SCs can also be used to make cheaper, quicker and more secure mortgage-based transactions. This will allow buyers to access purchased real estate more quickly as well as making the whole process smoother. "Smart" mortgage contracts will allow both sides to settle purchases in digital form before processing payments. As soon as this happens, information about property rights is updated in the SC to reflect the change of ownership. Insofar as the process requires the initial owner to input a unique key, it will be a lot more secure and less prone to fraud.

Insurance. The insurance industry spends tens of millions dollars annually to process claims. Moreover, it loses millions of dollars on account of fraudulent claims.

In addition to providing support for creating insurance policies, SCs can be used to check for errors and calculate insurance payments on the basis of a set of criteria that reflect the insurance terms for an individual or corporate policyholder. Thus, faster processing, a drastic reduction in errors, and smaller expenses are among the key advantages of using SCs in insurance.

In the longer term, SCs can be used for IoT-based transport vehicles, making possible "pay on delivery" insurance policies and the immediate filing of claims after accidents. Such information as driver's licenses, car documents, and accident reports can be processed immediately in order to speed up payments, which will benefit both parties. Theft, accident and other claims can be filed automatically, guaranteeing rapid client compensation. The client's driving habits can also be used to calculate insurance premiums and make rebates. Useful data for developers include the respect of speed limits, mileage, car maintenance schedule, brake use, point of collision, and road quality.

Home insurance. The SC technology allows the connection of smart home appliances such as refrigerators, thermometers, stoves and alarm systems. Their IoT data may trigger automatic insurance payments for claims connected to fire, theft or property damage. Claims linked to weather or earthquakes can also be automatically checked and paid with the help of alarm systems, eliminating the cumbersome process of manual verification.

Medical insurance. Insurance companies can make use of developments in biotechnologies and IoT (smartwatches) to create SCs that would offer rebates on medical insurance or issue fines on the basis of information about the patient's health. Useful data include body weight, pulse, and possibly even more complex biometric information in the future. SCs can also be used to uncover anomalies that require medical consultations if the patient wants to continue to benefit from favorable rates.

Flight insurance. Web APIs such as Flight Stats and Aviation Edge provide minute-by-minute information about flight delays and cancellations. Programs such as Chainlink[15] can update SCs on the status of flights to determine whether policyholders should receive compensation.

Insurance and reinsurance of large equipment. Many companies make use of large expensive equipment for their business operations. The

[15] Chainlink is the first decentralized oracle network that gives smart contracts decentralized bidirectional possibilities to receive external inputs and send outputs to other systems. Available at: https://blog.chain.link/44-ways-to-enhance-your-smart-contract-with-chainlink/ (accessed: 2.08. 2019)

key mechanisms of such equipment can be provided with IoT devices for gathering real-time information about their state. Programs such as Chainlink can transmit such data to SCs for making insurance payments for failures or scheduled maintenance. As policies for large equipment are usually reinsured, Chainlink can be used to distribute claims and client payments between all insurance providers.

Supply chains (from procuring materials to delivering goods to the end user) are another business sector that can benefit from blockchain-based SCs. IoT devices can be used throughout the entire supply chain in order to record a product's every step. SC-based smart supply chains may theoretically eliminate internal theft, as managers will be able to track missing products to the precise time and place where they disappeared.

In large supply chains, SCs will allow managers to keep track of supplies in real time and calculate the time needed for products to pass through the whole chain. Managers will be able to use this information for adjusting supply levels and developing new working methods for accelerating deliveries.

For supply chains distributed across different places, SCs can be used to do all of the above as well as to initiate automatic reorders and payments of already received orders. The information contained in SCs can also be used for calculating future traffic in supply chains and even the products that should be stored in warehouses at different times of year.

Retail payments. Many popular user apps such as Uber and Airbnb allow clients to make retail payments with the help of SCs by giving the latter access to major credit cards and payment networks (PayPal and Stripe).

Public utility payments. Water, electricity and Internet may be called the foundations of modern society. Public utilities largely use outdated infrastructure and technologies for assuring security. SCs make it possible to modernize vital infrastructure by adapting and connecting outdated systems to blockchains.

Some public utilities such as Internet and cable TV collect regular lump-sum payments from their clients. However, when their services are disrupted, no one is held responsible. IoT devices can monitor the time of the faultless operation of public utilities, and programs such as Chainlink can input this data into SCs for calculating monthly payments or paying compensation for periods of inactivity.

IoT devices can also calculate the consumption of companies and individual users. Chainlink can incorporate consumption norms into SCs

in order to initiate fines for excessive consumption, generate electricity bills, or collect carbon taxes. People can also sell their energy back to the Network for profit. SCs can record the readings of smart meters for monetizing output and facilitating payments for both energy consumers and producers. Solar panels, Tesla Powerwalls and wind turbines are examples of new energy sources that can be linked to SCs.

Waste management. Emissions and waste disposal are two sectors that can be transformed by SCs connected to IoT devices that make precise measurements of output volumes. Such data can automatically initiate payments to the respective regulatory body or monetize waste that is consumed during recycling or the conversion of waste to fuel.

Quality control. IoT devices can be used to verify the authenticity and proper maintenance of products over the whole supply chain. Examples include storing products at prescribed temperatures, verifying the hermeticity of containers, and tracking the location of goods. SCs can initiate payments and impose fines depending on whether the output of IoT devices confirms the respect of quality control standards as defined in the contract.

Voting and polls.[16] Despite the use of computer systems costing millions of dollars, malfeasants still manage to rig voting results. SCs represent a simple and economically effective solution for assuring trust and transparency in this area. They can be used to confirm voters' identities and record their votes. This information can be used to trigger actions after voting results are tallied. As blockchain blocks cannot be changed after they are recorded, it is impossible to manipulate such results.

Personal data. SCs can also be used for biometric data such as fingerprints or eye scans. As biometric data are unique, they can provide an effective means of identifying people if there exists a reliable database or source for cross-referencing it. Oracles can deliver biometric data to SCs and connect the latter to different databases for authentication.

The concept of "decentralized identity" has been made possible by DLT apps. Personal data can be stored in a blockchain rather than in a public or private centralized repository. SCs can use such databases with the help of oracles for verifying registration data such as name and citizenship without leaking

[16] Opinion, a Russian-language social networking service, conducts polls and forecasts the outcomes of events with the help of "collective intelligence." Based on the EOS blockchain, the project was launched in early 2019 and has continued to develop ever since. For conducting polls, Opinion uses an SC that automatically records user responses in the blockchain. Available at: https://bits.media/oprosy-i-golosovaniya-na-blokcheyne-neizmennost-i-prozrachnost-rezultatov/ (accessed: 2.08.2019)

personal information. In the future, such databases may be consulted by SCs for verifying voting results, checking KYC/AML, and passing customs.

In fact, the list of sectors that can benefit from the new technology is enormous. Given that SCs support and assure the secure development of products, these sectors can range from small startups to technology giants such as Microsoft or Amazon.

SCs can ultimately put an end to our dependence on banks. Another major benefit is that they can make our world more democratic. As they can be used for exchanging both simple things (e.g., labor) and more complicated entities (e.g., credits), the number of such services will undoubtedly grow exponentially over time.

5. Risks of using smart contracts

The technological advantages of SCs can help to speed up transactions, lower costs, and simplify and streamline processes. At the same time, it must be admitted that the use of the still developing SC and blockchain technologies is fraught with a number of potential risks, including risks of management, deployment and regulation, legal risks, and risk management.

The decentralized model creates problems for changing rules insofar as such changes must be agreed to by all parties for the SC to function. Moreover, things aren't as optimistic as they might seem: a Europol report[17] suggests that terrorists, who receive the bulk of their financing through ordinary money transfers today, may begin to use SCs for organizing attacks and other illicit activities in upcoming years.

The reliability of SCs also evokes doubts. Fraudulent schemes and financial pyramids are already being organized with the help of SCs. Some key drawbacks of the introduction of SCs include

The early phase of development of SCs and blockchains turns away individual consumers, companies and governmental agencies. The complexity of these technologies and their associated risks make people suspicious insofar as they are accustomed to writing hard-copy documents setting down the rights and responsibilities of parties and signing them by hand.

Uncertain regulatory framework: it is not yet clear how SCs will be governed by law. For this reason, their recognition by courts could have

[17] Terroristy i smart-kontrakty. Evropol vypustil trevozhny otchet [Terrorists and smart contracts: Europol publishes an alarming report]. Available at: https://www.rbc.ru/crypto/news/5ba3aa4a9a794711b661ebdd (accessed: 2.08. 2019)

a decisive impact on the development of apps that would help to avoid undesirable legal consequences.

Errors: if the computer code does not precisely match the parties' intent or simply contains programming errors, the system might not execute as expected.

Rigidity: the basic idea is to agree on conditions that would be automatically implemented. However, the parties must foresee future scenarios that may require changes.

Rather than being eliminated, third parties will begin to play new roles. For example, experienced lawyers will consult clients on creating new contracts.

Our analysis of the potential risks of introducing SCs into economic and other social relations points to the existence of the following groups and types of risks:

legal risks (legal indeterminacy, contradictory or insufficient court precedents, etc.);

technological risks (peculiarities of software, etc.);

operational risks (role of the human factor (personnel) in applying computer technologies, etc.);

criminogenic risks (use of SC technologies for embezzlement and other crimes).

Conclusion

It is important to pass from the legal definition of SCs, the description of their legal and technological aspects, and the enumeration of their advantages and disadvantages to the creation of startups in a wide range of areas, including business, state control, and social relations. Research and informational support for the theoretical and practical results of such processes shall promote the development of diverse sectors of the economy, public governance and digital technologies and improve the quality of life of citizens and society as a whole.

To be effective, SCs and blockchains require a set of standards or general rules for all participants in order to assure accuracy and precision. Blockchain management standards will ultimately strengthen market confidence in these technologies and their regulatory framework. This will accelerate the diffusion and success of SCs.

To sum up, blockchain-based SCs aim to change the way contracts function. Many companies and governments are working on these tech-

nologies in view of the advantages they can provide (lowering costs, raising security, increasing speed and, of course, confidence). However, key drawbacks inhibiting their broad use include their early development phase and especially the ambiguity of whether they shall be governed by existing laws or require additional regulations. For the time being, these technologies shall be limited to certain business sectors such as banking and insurance rather than being used by private individuals. We believe that SCs shall not replace traditional contracts: rather, they will provide some sectors with alternatives that can give considerable benefits.

Current approaches to the legal regulation of SCs are in keeping with existing principles of contract law. They provide a number of legal and technical remedies and encourage legislators and lawyers not to overlook SCs as useful tools for assuring legal security. SCs are self-executing contracts that, in a certain sense, can be viewed as spinoffs of electronic data exchange. Their automatic execution is often implemented through computer code that translates legal language into a self-executing program that exercises control over relevant material and digital objects. SCs may be called sets of programmable computer functions that can self-execute upon the fulfillment of certain conditions.

Thus, a decentralized blockchain-based SC is a digital agreement that (a) is written in computer code (software), (b) runs on blockchains or similar distributed ledger technologies (decentralized), and (c) executes automatically without the need for human interference ("smart").

There are two approaches to legally defining the SC. One is to call it a type of contract. Such a contract becomes legitimate, it is protected by existing law, and the SC (code) can be used as electronic evidence. The other is to view the SC not as a separate type of contract but as a means of formatting an agreement between economic actors using the blockchain technology in order to save time and technical and material assets and to lower or eliminate legal risks for the parties. To this end, one can use either a wait-and-see approach or a "sandbox" for regulating SCs and the blockchain technology as a whole. The blockchain space is constantly developing and altering course in an unpredictable manner so that one should be wary about regulating things that have not been fully understood so far.

The following initiatives are necessary for developing a legal framework for SCs:

studying the legal consequences of the discovery of an intentional error in translating contract terms into computer code: will they differ from the consequences of unintentional errors?

enforcing the execution of automatic terms — in particular, through enforcement or bankruptcy proceedings;

studying the possibility of publishing an official list of contract types that can contain self-executing terms;

prohibiting contracts requiring state registration from containing self-executing terms;

assigning responsibilities to parties for errors in the computer code and introducing procedures for mitigating the consequences of errors, hacker attacks, and force majeure (in particular, by the decision of the court) and protecting from fraud, blackmail and other unlawful intentions (by recognizing an agreement as void and applying the consequences of invalidity);

solving the problem of presenting documents with contract terms to courts, tax authorities and other public agencies.

Developing a mechanism for demonstrating the unambiguous consent of the contractual parties to the terms of the SC and for assuring courts that these parties had been sufficiently informed about the contractual terms. There are two possible approaches to this issue: stakeholders should either develop SCs to bring them into line with existing law or develop new laws that would address the legal fine points of SCs. The use of closed key cryptographic signatures as a means of "signing" SCs should be considered objective proof of acceptance, intention and mutual agreement simultaneously.

Internet courts should recognize submitted digital data as evidence (recognition of digital objects as new types of evidence) if the parties collect and store this data on a blockchain with digital signatures and reliable time tags or on a digital platform and can prove the authenticity of the employed technologies. In some cases, it may be necessary to conduct technical expert evaluations or recruit specialists who would prove that an entry in the register was indeed made by a specific person at a specific time. Evidence that is authenticated and presented with the help of blockchains should be considered admissible in legal cases.

References

Anisimov V.F., Sergevnin V.A. (2018) Robotics and automation: legal education and profession. *Yuridicheskoye obrazovaniye i nauka*, no 3, pp. 11–16 (in Russian)

Bashir I. (2017). *Mastering blockchain*. Birmingham: Packt, 531 p.

Chandler S. (2019) Smart contracts are no problem for the world's legal systems, so long as they behave like legal contracts. Available at:

https://cointelegraph.com/news/smart-contracts-are-no-problem-for-the-worlds-legal-systems-so-long-as-they-behave-like-legal-contracts (accessed: 10.06.2020)

Dolova M.O. (2019) The question of applicability of blockchain technology in the consideration of cases by courts. In: Yu. V. Truntsevsky (ed.) Legal regulation of contractual relations arising in connection with development of digital technologies (smart contracts). Round table proceedings. Moscow: Jurist, pp. 27–36 (in Russian)

Efimova L.G., Sizemova O.B. (2019) Legal nature of the smart contract. *Bankovskoye pravo*, no 1, pp. 23–30 (in Russian)

Gatteschi V. et al (2018) Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, no 10, p. 20.

Golovanova N.A., Gravina A.A., Zaitsev O.A. (2019) *Criminal activity in the conditions of digitalization.* Moscow: Kontrakt, 212 p. (in Russian)

Grigg I. (2004) The Ricardian contract. In: *Proceedings of the First IEEE International Workshop on Electronic Contracting*, pp. 25–31.

Gromova E.A. (2018) Smart contracts in Russia: an attempt to determine their legal essence. *Pravo i tsifrovaya ekonomika*, no 2, pp. 34–37 (in Russian)

Ivanov A.Y. et al. (2017) Blockchain at the peak of HYIP: legal risks and opportunities. Moscow: Higher School of Economics Publishing House, 237 p. (in Russian)

Kalinina A.L. (2019) Issues of using smart contracts. In: Legal regulation of contractual relations arising in connection with development of digital technologies (smart contracts). Round table proceedings, pp. 37–45 (in Russian)

Kamalyan V.M. (2019) Concept and legal features of smart contracts. *Yurist*, no 4, pp. 20–27 (in Russian)

Khabrieva T.Y., Chernogor N.N. (2018) Law in the conditions of digital reality. *Zhurnal rossiyskogo prava*, no 1, pp. 85–102 (in Russian)

Khabrieva T.Y. (2018) Law before the challenge of digital reality. *Zhurnal rossiyskogo prava*, no 9, pp. 5–16 (in Russian)

Makarchuk N.V. (2019) Public law restrictions on the use of digital assets and technologies. *Predprinimatel'skoye pravo*, no 1, pp. 40–43 (in Russian)

Nagrodskaya V.B. (2019) *New technologies (blockchain / artificial intelligence) at the service of law.* Moscow: Prospekt, 128 p. (in Russian)

Navarro N. et al (2017) *Inteligencia artificial*. Valencia: Tirant, 293 p.

Nosov S.I. (2019) Law and informatization. *Yurist*, no 4, pp. 6–13 (in Russian)

Parfenov A.V., Shapovalov I.M., Valko D.V., Kirillov A.A. (2015) *Logistics of e-commerce*. Saint Petersburg: State Economic University, 79 p. (in Russian)

Perov V.A. *(*2017*) Identification, qualification and organization of investigation of crimes committed with the use of cryptocurrency.* Moscow: Yurlitinform, 177 p. (in Russian)

Popova E.M., Popov N.V. (2016) Blockchain as a driver of change in the banking sector]. *Bankovskiye uslugi*, no 12, pp. 9–14 (in Russian)

Rassolov I.M., Matytsina T.V., Yanenko M.B. (2006) *Legal issues of Internet relations.* Moscow: Yuniti, 165 p. (in Russian)

Ream J., Chu Y., Schatsky D. (2016) Upgrading blockchains: Smart contract use cases in industry. *Deloitte University Press*, no 4, pp. 1–11.

Savelyev A.I. (2016) Contract law 2.0: "Smart" contracts as the beginning of the end of classical contract law. *Vestnik grazhdanskogo prava*, no 3, pp. 32–60 (in Russian)

Savelyev A.I. (2017) Some legal aspects of using smart contracts and blockchain technologies under Russian law. *Zakon*, no 5, pp. 94–117 (in Russian)

Shaidullina V.K. (2019) Smart contracts on the financial market: research results. *Sud'ya*, no 2, pp. 21–23 (in Russian)

Sinitsyn S.A. (2019) The agreement: new aspects of legal regulation and interpretation. *Zhurnal rossiyskogo prava*, no 1, pp. 45–61 (in Russian)

Stark J. (2016) Making sense of blockchain smart contracts. Available at: https://www.coindesk.com/making-sense-smart-contracts/ (accessed: 20.05.2018)

Tjong Tjin Tai E. (2017) Formalizing contract law for smart contracts. Available at: https://ssrn.com/abstract=3038800 (accessed: 20.05.2018)

Volos A.A. (2018) Smart contracts and principles of civil law. *Rossiyskaya yustitsiya*, no 12, pp. 5–7 (in Russian)

Wattenhofer R. (2016) The science of the blockchain. Create Space Independent Publishing Platform, 131 p.

Yanenko M.B., Yanenko M.E. (2015) Methodology of elaborating marketing strategies in the conditions of using information and digital technologies. Saint Petersburg: State Economic University, pp. (in Russian)

Zemtsov A.N. (2016) Blockchain for all. *Otkrytye sistemy,* no 4, pp. 24–26 (in Russian)

Criminal law treatment of deviant behavior in media and social networks

Yulia Gracheva

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: uvgracheva@mail.ru

Sergey Malikov

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: s.v.malikov@yandex.ru

Alexander Chuchaev

Professor, Chair of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: moksha1@rambler.ru

Abstract

It would be difficult to imagine modern society without information and telecommunication networks, including media and social networks that promote the development of the economy, education, medicine, etc. Media and social networks are an important means of communication and especially so during the coronavirus lockdown; however, the more people are involved in cyberspace, the more crimes are committed there. The subject of this study is deviant behavior on media and social networks with the objectives of identifying the main types of deviant behavior, ascertaining the techniques used to impair public relations protected by criminal law, assessing the existing measures in criminal law that prevent deviant behavior on the internet, and proposing new measures that may be necessary. General scientific (dialectical, logical, systematic) and special legal (comparative legal, formal legal, legal modeling) methods are applied. More than 80% of cybercrime in Russia involves theft using modern social engineering technology for phishing. Although the Supreme Court of the Russian Federation has recommended otherwise, these thefts are treated as a different class in the theory of criminal law and judicial practice. One of the ways to achieve uniformity in law enforcement is to exclude special types of fraud from the Criminal Code of the Russian Federation. Another common way of taking possession of someone else's property is to use a computer program to freeze a system until a certain amount of money has been transferred to a particular account. A gap in the treatment of such acts by criminal law is identified and ways to eliminate it are proposed. The 2020 pandemic highlighted the role of internet in spreading various pieces of fake news; Federal Law No. 100-FZ of April 1, 2020, which supplemented Articles 207.1 and 207.2 of the Criminal Code, was an effective

and timely response. Media and social networks are often used as a platform for inciting, preparing and/or organizing the commission of a crime or other offenses. The study of cyberterrorism shows that there is no need to introduce an independent standard for such acts. Cybercrime also includes attacks on privacy, and the article explores internet harassment in detail by delineating different types of it and the legal response to them. A proposal to amend the wording of Article 137 of the Criminal Code is judged sound.

Keywords

media and social networks; deviation; criminal liability; fakes; phishing; cyberbullying; computer fraud; privacy; cyberterrorism.

Acknowledgments: The work was supported by the RFBR (research project No 18-29-16158)

For citation: Gracheva Yu. V., Malikov S.V., Chuchaev A.S. (2021) Criminal Law Treatment of Deviant Behaviour in Media and Social Network. *Legal Issues in the Digital Age,* no 1, pp. 123–144.

DOI: 10.17323/2713-2749.2021.1.123.144

Introduction

A number of factors make committing crimes in the digital realm tempting. First, its illusion of anonymity and therefore impunity removes the fear of punishment and increases the likelihood of unlawful behavior. Second, the transnational aspect of such criminality together with online access from anywhere in the world means that where a crime is committed may have nothing to do with where the perpetrator is; preparing for a crime and committing it can be coordinated among participants from different parts of the world. Third, over 4.5 billion people are in cyberspace.[1] Fourth, artificial intelligence may be used to commit crimes [Van der Wagen W., Pieters W., 2015: 578]. Fifth, exchange of information is practically instantaneous. Sixth, any necessary information can be collected without calling attention to oneself; this could even include material about potential targets for acts of terrorism and the persons who could carry them out. Seventh, the financial system for digital accounts is uncontrolled, and the transactions that underwrite crimes can be executed anonymously. Finally, detecting and investigating these crimes is difficult and may lag far behind the time when they are committed.

[1] Interpol-Europol 8th Cybercrime Conference: Half of humanity at risk. Available at: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-Europol-8thCybercrime-Conference-Half-of-humanity-at-risk (accessed: 2 February 2021)

Some distinguishing features of deviant behavior in the digital realm are: use of information and telecommunication networks, and in particular media and social networks, which is typically accompanied by illegal access to electronic information; the creation, use and distribution of malware; and violations of the rules governing use of storage, of processing or transmitting electronic information and of information and telecommunication networks.

Over 80% of Russian cybercrime in 2019 involved some form of theft; more than 8% involved illegal sales of narcotics (Article 228.1 of the Criminal Code of the Russian Federation (further, CC RF); and about 1% consisted of crimes involving electronic information. Ministry of Internal recorded 508 personal privacy violations (Art. 137 of the CC RF); 469 crimes related to extremism (Art. 205.2 and 208); 232 violations of copyright and related rights (Art. 146); and 25 suicide-related incidents (Art. 110 and 110.1) [Kirilenko V.P., Alekseev G.V, 2020: 900]. As is the case in all European countries, 80% of cybercrime is prompted by motives of self-interest.

It seems important to identify the basic types of deviant behavior on the internet, understand the hazard they present to society, judge how they fit into the existing legal and regulatory framework, and propose pertinent solutions if there are lacunae. A combination of general scientific and specialized legal research methods will be used to these ends.

1. Phishing — theft or computer fraud?

A substantial number of acts detrimental to society which are committed through social networks involve fraud [Solov'ev V.S., 2016: 60]. Phishing, which is one of the widespread techniques for social engineering, is used to commit fraud by gaining access to confidential user information — logins and passwords. If an email sent as part of a phishing attack contains a link to a counterfeit webpage that precisely mimics the form and content of an official interface and requires entering confidential information (a debit card number, PIN code, etc.),[2] then that theft of property is subject to criminal liability for theft of a bank account (or theft of electronic funds) under Art. 158(3)(d) of the CC RF.

Phishing emails may contain various kinds of programs (trojans) that are installed without permission on the victim's computer, smartphone or other high-tech device if the e-mail is read and the links in it are followed.

[2] How to Recognize and Avoid Phishing Scams. Available at: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (accessed: 2 February 2021)

All the recent bank trojans written for Android are able to divert money automatically.[3]

Some legal scholars of the matter maintain that this method for misappropriating funds has not been properly addressed in the CC RF, even though there are such points as Art. 158(3)(d) and Art. 159.3 and 159.6. They propose supplementing the Code with a separate "form of theft involving a new way of committing it by employing computer technology" [Inogamova-Hegai L.V., 2019: 55]. That proposal might have merit if the legislation had not provided differentiated liability for theft that hinges upon the method use to misappropriate someone's property (Art. 158–162). However, in accordance with the rules for classification under general and special standards, liability would be incurred by committing an act specified by a special standard (for the matter in question that would be Art. 158(3)(d) and Art. 159.3 and 159.6), which renders such proposals pointless. Finally, the legislature has in essence already carried out a related proposal by passing Federal Law of 29 November 2012 No. 207-FZ "On amending the Criminal Code of the Russian Federation and certain legislative acts of the Russian Federation"[4] which inserted Art. 159.6 "Fraud in the field of electronic information" into the CC RF. Despite its title, the crime that Art. 159.6 addresses is not fraud but a separate type of theft with its own methods for misappropriating property or the right to it [Bolsunovskaya L.M., 2016: 15]. Those methods include inscription, deletion, blocking and modification of electronic information or other interference with the functioning of storage devices, with processing and transmission of electronic information, or with information and telecommunication networks. As justification for our position that Art. 159.6 of the CC RF addresses a separate type of theft, we may first cite the first para of the Resolution of the Supreme Court of the Russian Federation of 30 November 2017 No. 48 "On judicial practice in matters of fraud, misappropriation and embezzlement".[5] Its list of the articles of the Criminal Code of the RF, which pertain to fraud omits Art. 159.6. Then, the method of misappropriation of property that distinguishes fraud from other kinds of theft is deception or abuse of trust which causes the victim to transfer their property or the right to it, that is, "there must be a victim of 'deception'" [Kibal'nik A., 2018: 67]. That deception is lacking in the case of computer

[3] Chernykh E. Cybercrime and our telephones. Available at: http://crimescience.ru/?p=9980 (accessed: 2 February 2021)

[4] Collected Laws of the Russian Federation. 2012. No. 49, item 6752.

[5] Bulletin of the Supreme Court of the Russian Federation. 2018. No. 2.

fraud because the victim is unaware of the method for misappropriating the crime's target object [Lopashenko L.A., 2015: 507].

This issue came up when a person identified as Z., who was employed as a sales consultant at the Volga branch of Togliatti regional office of the Megafon mobile phone chain, was convicted under Art. 159.6(1) of the CC RF of modifying the electronic information in the SBMS program used to serve mobile phone subscribers. Z. has transferred illegally funds from personal accounts that belonged to Megafon Company. This computer fraud resulted in theft of 500,699.97 rubles.[6]

The materials in this criminal suit make clear that there was no deception of the victim that would have caused them to independently transfer funds to the guilty party. Furthermore, the courts of the first and appellate instance found no evidence in Z.'s acts of the crime specified in Art. 272 of the CC RF. The court of first instance concluded that Z.'s criminal acts were fully consistent with the offense specified in Art. 159.6 (1). The illegal access to electronic information that Z. obtained for the purpose of carrying out the criminal intent to divert funds from Megafon consisted of acts that constituted the objective aspect of Z.'s fraud as specified in Art. 159.6 (1).[7]

The bodies charged with preliminary investigation of Z.'s acts were commissioned under Art. 272(3) and 159.6(1), which is consistent with the elucidation contained in para 20 of the Decision of the Plenum of the Supreme Court of the RF of 30 November 2017 No. 48. The presidium of the Samara Oblast Court called attention to that circumstance when it responded to the cassation appeal of the victim and the prosecutorial presentation by referring the case for a new trial.

There are two points of interest in the verdict rendered. The first is that not all legal scholars and law enforcement agencies find it obvious that those acts meet the criteria for multiple offenses in accordance with the relevant sections of Art. 159.6. and 272–274 of the CC RF [Kibal'nik A., 2018: 67].[8] They would maintain that computer crimes are a method of committing fraud involving electronic information and that, therefore, those acts were not multiple. The second is that it would be difficult to agree that the acts meet the criteria of Art. 159.6(1) of the CC RF because there is no

[6] Decision of the Presidium of the Samara Oblast Court. 14 February 2019 No. 44U-36/2019, 44U-37/2019 // SPS Consultant Plus.

[7] Ibid.

[8] Verdict of Kaluga Regional Court. 9 August 2017. Case of B. In: Criminal jurisdictional activity under digitalization. Moscow, 2019, p. 114.

victim of deception, and it is no less difficult to accept the existing standard and the explanations of the practices for applying it provided by the Plenum of the Supreme Court of the RF.

Distinguishing between several special types of fraud and theft is a problem that has come up both in theory and in practice, and it has not been solved by the passage of Federal Law of 23 April 2018 No. 111-FZ "On amending the Criminal Code of the Russian Federation" which inserted para. 3 into Art. 158 of the CC RF and para 3 and subparagraph d into Art. 159.6 of the CC RF (theft and fraud, respectively, with respect to money "from a bank account and equally with respect to electronic funds") and clarified the title and content of Art. 159.3(1) of the CC RF as fraud by means of electronic execution of payment.[9] Our view is that this in fact blurred the distinction between theft from a bank account (Art. 158(3) (d) and fraud by means of electronic execution of payment (Art. 159.3) and computer fraud (also Art. 159.6). Some authors maintain that it has been difficult to find characteristics that would set theft from a bank account apart from general criminal fraud employing information and communication technologies and electronic execution of payment (Art. 159) [Russkevich E., 2019: 60]. If a perpetrator took possession by any means of the debit card and personal information of a victim and, for example, withdrew cash from an ATM and then made a wire transfer from the victim's card to someone else's account, that act would certainly meet the criteria of Art. 158(3)(d) of the CC RF. Ivan Klepickij takes a diametrically opposed position that this would be an instance of the crime specified by Art. 159.3. "The current version of the law does not require for the application of Art. 159.3 that there be a victim of deception, and the manner of committing the crime is likewise not specified" [Klepickij I.A., 2021: 357]. His position has at times been upheld in judicial practice. For example, a person who found a wallet with two bank cards and spent 12,984.31 rubles via contactless payments was convicted under Art. 159.3.[10] However, the Cheryomushki District Court of Moscow arrived at opposite conclusion in its verdict that Art. 158(3) (d) applied to the actions of an automobile driver who transferred funds to his own bank card from a mobile phone with its mobile banking interface still open that someone had left in a rear passenger seat compartment.[11]

[9] Collected Laws of the Russian Federation. 2018. No. 18, item 2581.

[10] Verdict of the Graivoronsky District Court, Belgorod Oblast. 15 July 2019. Case No 1-40/2019.

[11] Verdict of the Cheryomushki District Court of Moscow. 15 July 2019. Case No 1-387/2019.

The same classification should apply to manipulation involving electronic information through which a person gains access to someone's bank account (by social engineering, for example) and then arranges wire transfers of funds from the victim's account to their own or to another person's. Clearly cases of this kind should incur criminal liability not only for theft (Art. 158(3)(d) but also for crimes involving electronic information (Chapter 28 of the CC RF). The classification would be no different even when "manipulation involving electronic information (inscription, modification, etc.) does not result simply in movement of funds, but also when it disrupts normal operations in the information and communications infrastructure (such as blocking a personal user account in a system for providing remote services)" [Russkevich E., 2019: 61].[12] In these situations, the method used to misappropriate someone's property is unchanged and remains concealed.

Art. 158(3)(d) of the CC RF and that article as a whole, which together prescribe liability for computer crime, should also apply to acts of a perpetrator who uses a trojan computer program to obtain remote access to a system (a personal computer, mobile banking, etc.) and then to install programs that control the keyboard and mouse in parallel with the system's operator in the event that the illegitimate access to information has been used to misappropriate someone's property.

It follows that neither Art.159.6 nor Art. 159.3 cover theft through electronic execution of payments or involving electronic information as a way to seize someone's property because any deception or abuse of trust which causes the victim to "voluntarily" give that property away is absent. The proposal in this connection would be, first, to classify theft of another person's property according to legislation that delineates the forms of theft. This would make Art. 159.6 superfluous. The second part of the proposal would be to exclude any special content of fraud from the CC RF. Although this is not a new idea, it has become all the more pressing. It follows that retaining Art. 159.6 is inadvisable, first, because it does not solve the problem of one alternative for theft (Art.158(3)(d) competing with another in the section on theft involving electronic information. Second, the existence of special criteria should be justified by broader or narrower impositions of liability for the crimes that are established by them. However, the penalties for committing the acts specified by Art. 158(3)(d) and 159.6 debates over the necessity of criteria for the entire range of fraud involving electronic information and computer crimes.

[12] Russkevich maintains that this would be an instance of fraud involving computerized information.

2. Extortion via the internet: Gaps in regulation by criminal law

Ransomware is a type of computer program (trojan) contained in phishing emails. The program will block the operation of a computer and demand transfer of a certain amount of money to an account such as an electronic wallet as a condition for restoring the functionality of the system. It will also threaten to erase information kept on the computer if the demand is not met. These program codes are not designed to damage computers as such or their parts, but instead to erase information located in them. Acts of this kind incur cumulative liability: under Art. 272(2) (motivated by gain) or 272(4) if the consequences are grave or if there is a threat of such consequences; and under Art. 273 because creating and deploying harmful programs in not covered under Art. 272. Liability under Art. 273 is necessarily incurred whether the perpetrator wrote the harmful program or obtained it ready for use; this is because a socially hazardous act in Art. 273 may take alternative forms as creation, dissemination and use. This position has been confirmed by judicial practice.[13]

A demand that money be transferred with a threat to erase information (databases) cannot as such be classified under Art. 163 even though it is intended to misappropriate another person's property. Extortion is defined as a demand for the transfer of someone's property under threat of violence or of destruction or damage to someone's property, as well as threat of dissemination of information harmful to the victim's reputation, etc. According to Art. 128, in which ownership rights are defined in relation to property, information and databases are not considered property although they may be subject to civil rights [Danilov D., 2018: 37–42]. The fact that Art. 163 makes no reference to commission of a crime by threatening to erase information and thus hampers proper recognition of such acts by criminal law constitutes a problem, which must be eliminated by agenda to Art. 163(1) of the CC RF so that this kind of threat is specified.

3. Fakes on social networks

In February and March 2020 an intensive campaign of fakes concerning the coronavirus infection (COVID-19) was launched. It was intended to induce fear and panic in the populace, to give the impression that the

[13] For example, by the Appellate Decision of the Moscow City Court of 27 November 2020 in case No. 10-16199 // Consultant Plus.

country's leaders could not deal with the outbreak and were concealing important information, and to compromise and discredit law enforcement agencies, etc. As the World Health Organization acknowledged, a true "pandemic of fake news" or "infomedia" came along right after COVID-19 had taken off, and it spread across the planet even faster than the virus itself. Its main "carriers" were mobile platforms and, above all, the popular messaging service WhatsApp.[14]

The pandemic of fakes "blanketed" Russia too. The governor of Yamal had to intervene in order to debunk one of these fakes. On local networks rumors persisted that someone in the top management of a gas producing company went to Italy and, "didn't tell anyone about it or stayed in quarantine, and everyone in the town was exposed, which caused a coronavirus outbreak". Within a week that story seemed almost official. A fake circulated at about the same time in Ufa stated that a thousand graves were being prepared somewhere in the vicinity to accommodate coronavirus deaths. In the town of Chebarkul in Chelyabinsk oblast one woman claimed in all seriousness that troops were dispatched to the city to suppress "food riots".[15]

To prevent mass dissemination of fakes that would cause panic and disturb public order, Federal Law of 1 April 2020 No. 100-FZ "On amending the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedural Code of the Russian Federation" was passed. It supplemented the CC RF with Art. 207.1 "Public dissemination of intentionally falsified information about circumstances that constitute a threat to the lives and safety of citizens" and 207.2 "Public dissemination of intentionally falsified information that leads to grave consequences".[16] This law came into force 1 April 2020.

Presidium of the Supreme Court of Russia has explained that fakes related to COVID-19 fall under Art. 207.1 because "spreading infection by the novel coronavirus (COVID-19) within the Russian Federation has currently and may in the future result in human suffering, harm to human health, substantial material losses, and disruption in the living conditions of the populace...."[17]

---

[14] Available at: https://rg.ru/2020/04/16/voz-obiavila-o-pandemii-fejkov.html (accessed: 23 April 2020)

[15] Available at: https://rg.ru/2020/04/18/reg-urfo/advokat-rasskazal-chto-zastavliaet-liudej-rasprostraniat-fejki-o-koronaviruse.html (accessed: 23 April 2020)

[16] Rossiyskaya gazeta. 3 April 2020.

[17] Review of selected issues in judicial practice as they concern application of legislation and measures to combat the spread of the novel coronavirus (COVID-19) within the Russian Federation. No. 1 // Consultant Plus

The actions of individual persons are evidence of criminally punishable acts under Art. 207.1 of CC RF in the event that they constitute public dissemination of seemingly trustworthy accounts of intentionally falsified information about circumstances that present a threat to the lives and safety of the populace, including about the circumstances associated with the spread of the novel coronavirus (COVID-19) within the Russian Federation or circumstances associated with the protective measures, techniques and methods adopted to ensure the safety of the populace in those circumstances. If spreading such falsehoods constitutes an actual hazard to society and harms public safety and order, then criminal liability is incurred.

Socially significant information may also include information about the circumstances that constitute a threat to the lives and safety of the population and/or about the protective measures and methods adopted in order to ensure the safety of the population and territory in such circumstances.[18]

If fakes result in someone's death or harm to their health, then the acts would fall under Art. 207.2.

Various social networks are typically involved in disseminating such information, as review of both Russian and international practices will show.

Social networks are monitored on a daily basis in order to prevent the spread of such information. The materials that turn up are vetted, and if any information about circumstances that constitute a threat to the lives and safety of the populace is intentionally falsified, then Roskomnadzor will block it. For example, internet monitoring discovered a report alleging that those who died of the coronavirus were being removed by night from an observation center in Krylatskoye. Official information, however, stated that the observation center was being used to quarantine healthy people who had to leave self-isolation because of contact with someone infected. The Moscow City prosecutor followed up with an investigation concerning the fact of publication. The materials were turned over to the Investigative Committee for a determination of whether to lodge a criminal suit under Art. 207.1.[19]

A video clip with the headline "COVID-19 is transmitted by testing" on YouTube was discovered. The originator claimed that "the coronavirus was developed in the laboratory from a virus in bats, which was not transmissible between humans. It is carried to human beings by the testing

[18] Ibid.

[19] Available at: https://rg.ru/2020/04/18/genprokuratura-obnaruzhila-resursy-rasprostraniaiushchie-fej-ki-o-koronaviruse.html (accessed: 23 April 2020)

because 15–20% of tests are infected. Air-borne particles do not transmit it." The Prosecutor General found that the video stating that infection is the result of testing could convince people to reject testing and delay getting prompt assistance for severe infection. The originator of the clip was charged with a crime specified by Art. 207.1. On the official site devoted to combating coronavirus infection, information is posted about how it is transmitted by air-borne particles. This and other circumstances confirm the dissemination of intentionally falsified information.

4. Incitement to crime via media and social networks

Another risk arising from media and social networks is their use as platforms for inciting, preparing and/or organizing crime or unlawful acts.

On 23 and 31 January 2021 unlawful demonstrations showed evidence of using the internet, the social networks TikTok, VKontakte, Facebook, Twitter, Instagram, and the YouTube service to organize public disorder, spread slander, and persuade minors to commit acts that, at minimum, would constitute a hazard to their lives.

In the middle of that week Roskomnadzor required social networks to suppress solicitations to participate in the demonstrations. The Prosecutor General in turn insisted on imposing a complete ban on access to the websites that published such solicitations.[20]

It was observed that the irregular opposition in this instance turned to schoolchildren and not merely to secondary school students, but also younger children, and that it provided them with detailed instructions on how to behave at the demonstration, including extracting the SIM cards from telephones taken to the demonstration.

Roskomnadzor reported that moderators at VKontakte and YouTube deleted about 50% of total unlawful content that came to their attention. The TikTok app removed 38% and Instagram 17% of such data. Criminal cases under Art. 151.2(2)(c) of the CC RF (inciting minors on information and communication networks to commit acts that present a threat to their lives) were opened. In addition, the acts of the organizers and individual participants of unauthorized demonstrations could be charged under Art. 212.

Several researchers have found that al-Qaida, for example, is relying much more frequently on the digital communication platforms of Tele-

[20] Available at: https://rg.ru/2020/04/18/genprokuratura-obnaruzhila-resursy-rasprostraniaiushchie-fejki-o-koronaviruse.html (accessed: 23 April 2020)

gram and Signal. Jihadists prefer Twitter and Facebook to spread ideological propaganda. Cyberextremists rely heavily on the apps and programs of WhatsApp, Threema, Kik, Wickr and SureSpot to exchange messages.[21] As one example, a person identified as S. was convicted under Art. 205.2(2) of the CC RF of using the internet to call publicly for terrorist activities and publicly justify terrorism. The court acquitted S. of the charge of terrorist propaganda. The Judicial Collegium for Servicepersons changed that verdict and found that S.'s actions came under Art. 205.2(2) as public calls for terrorist activities, public justification of terrorism, and terrorist propaganda committed via the internet.

The court of first instance acquitted S. of terrorist propaganda on the grounds that the actions of the accused were not systematic in nature. However, that court's conclusion stands in contradiction to the materials introduced in the case and hinges upon an incorrect application of criminal law. By note 1.1 under Art. 205(2), terrorist propaganda is activity which disseminates materials and/or information aimed at indoctrinating a person with terrorist ideology, convincing them of its appeal or of the acceptability of terrorist action.

The hearings established that S. had three times posted for public viewing on his personal VKontakte page images, photographs and his comments on them which, according to the findings of experts, used psychological and linguistic techniques to incite violent acts (commission of acts of terrorism) against those who do not adhere to Islam; and in a second comment there were also justifications and approval of terrorist actions (armed jihad, and in particular as part of an international terrorist organization) as correct and objects for support and emulation.

The experts found also that material in the second comment affirmed the supreme importance of the pursuit of death by Muslims, approved of Muslims who had died in jihad, glorified the role of shahids, disapproved of non-Muslims, and spoke of the supreme value of fighting against "unbelievers" and the need to raise children within the traditions of that fight.

The acts of S. referred to in the verdict, the form and content of publications posted and openly accessible on the internet, his persistent intent to disseminate materials of a terrorist nature, and the testimony of witnesses concerning S.'s calls for acts of terrorist and public justification of terrorism — all these in sum show that he not only made public calls for acts of

[21] Is technology helping or hindering the fight against terrorism? Available at: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-thefight-against-terrorism/ (accessed: 15 March 2020)

terrorism and publicly justified terrorism, but that he also disseminated materials intended to inculcate an ideology of terrorism and a conviction that terrorism is appealing or that acts of terrorism are justified, which is to say that he engaged in terrorist propaganda.[22]

Terrorist propaganda, recruiting and training supporters, radicalizing a community, soliciting contributions, collecting information, arranging communication, and planning definite terrorist attacks through use of the internet are a hybrid form of cyberterrorism. In its pure form, it means actual attacks that usually target the critical information infrastructure of the Russian Federation in order to achieve political, religious or ideological objectives.

Some legal scholars regard the dissemination via internet of intentionally falsified information about impending terrorist acts as cybercrime (Kuleshova G.P., Kapitonova E.A., Romanovskij G.B., 2020: 161). In September 2017 there was an instance in Russia of dissemination of deliberately falsified reports of impending terrorism. It targeted the information databases of state institutions and caused damage appraised at over 300 million rubles. FSB Director Alexander Bortnikov reported that the four perpetrators were Russian citizens located abroad.[23] The media reported a version of events in which foreign special services had commissioned the attack to test a new method for hybrid warfare. In October 2018 the United Kingdom openly threatened Russia with a cyberattack on Moscow's electricity grid in the event of any aggression carried out against NATO or its allies.[24] Russia's special services have regarded acts of this kind as state terrorism.

Cyberterrorism has lately been the focus of increased attention. In the US and Western Europe cyberterrorism has mostly political connotations. Those countries peddle the notion that Russia, China and Iran pose a cyberthreat and promote the ideology that a cyberspace offensive against those countries must be mounted.

Criminal law studies on these topics are engaged in debate about how to increase liability for use of the internet to carry out terrorism. As always,

[22] Appellate Decision No. 225-APU19-1. Review of the judicial practice of the Supreme Court of the Russian Federation No. 1, 2020 // Bulletin of the Supreme Court of the Russian Federation. 2020. No. 10.

[23] Damage from telephone terrorism in Russia cost 300 million rubles. Available at: https://ria.ru/defense_safety/20171005/1506292428.html (accessed: 23 April 2020)

[24] UK war-games cyber attack on Moscow. Available at: https://www.thetimes.co.uk/edition/news/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0. (accessed: 23 April 2020)

opinions differ. One writer, for example, has proposed increasing the liability stipulated in Art. 205(2) for committing acts of terrorism by hacking into computer systems [Chekunov I.G., 2012: 43]. Others reject that suggestion on the grounds that the existing features of criminal law for counteracting cyberterrorism are sufficient [Kuleshova G.P., Kapitonova E.A., Romanovskij G.B., 2020: 163].

The latter position has merit, first, because a reading of Art. 205(1) of the CC RF indicates that it applies liability both for carrying out bombings, arson, etc. and also for the threat to do so. The mere threat is a less dangerous act than in fact setting off an explosion or arson; hence, an act of terrorism of that kind would incur penalties that are closer to the minimum prescribed in Art. 205(1). In such instances, circulating the threat via the internet does not require establishing that as a criterion and can be taken into consideration when a penalty is imposed under the sanction.

Furthermore, certain passages, such as some in Art. 205.2, have such a criterion.

5. Personal privacy in media and social networks

Media and social networks have become a convenient platform for carrying out internet harassment. In one fashion or another, harassment has affected half of all children. Adolescents who have been victims of harassment on the internet have usually been subjected to it beforehand in real life so that virtual harassment often exacerbates actual violence.

Along with adolescents, victims include public figures (actors, sport stars, people in show business, etc.) and former partners.

Internet harassment (cyberbullying) is defined as deliberate insults, threats, defamation or disclosure of compromising information to others by means of modern channels of communication and usually for an extended length of time. Along with "cyberbullying" such other terms as "internet mobbing" and "cyber-mobbing" for this phenomenon have been derived from English.

All forms of internet harassment share the following characteristics:

They are carried out online via information and communication channels, or via mobile phones through transmission of obscene video and audio clips, text messaging, or annoying calls. This enables: a) round-the-clock interference with privacy (attacks do not cease after the school or work day); b) unlimited geographic reach, which allows an unlimited audi-

ence and immediate dissemination; c) practical anonymity for the source of the messages or images that are transmitted electronically.

They are a form of persecution, i.e. illegal restriction of the right to life, health, free choice of residence, freedom of movement, etc., as well as a cause of moral damage, psychological trauma, and impairment of honor and dignity by insults, bullying, persistent slander, etc.

They are carried out for a long time as systematic acts characterized by some kind of harassment — circulating deliberate falsehoods (rumors and gossip) about a person, ridicule and provocations, direct insults and intimidation, shunning (boycotts and demonstrative disregard), attacks that impair the honor and dignity of a person and cause material or physical harm.

The victim typically does not know who is behaving aggressively because the perpetrator conceals their identity from the victim and can operate anonymously, which provides a feeling of impunity and often prolongs the attack. The victim's ignorance of the identity of the persecutor can contribute to feeling bullied, intimidated and upset.

"Internet bullying" is a phrase that refers first of all to cyberstalking, which consists of acts that disrupt personal privacy through persecution (telephone calls, emails, surveillance, etc.), persistent molestation, direct and indirect threats, gross insults and harassment. The case of a person referred to as G. is indicative in this regard. G. was accused of intentionally inflicting grievous bodily harm (Art. 111(2)(h) of the CC RF) and issuing death threats (Art. 119). When G. learned that his wife wanted a divorce, he stalked her, frequently threatened her and once took her to a forest where he placed a knife at her throat and demanded that she tell him about her relations with other men. She brought this to the attention of the police, but they would not issue criminal charges because tangible evidence of her husband's crime was lacking (although the fact that the accused had placed a knife at her neck might have been sufficient, even in the absence of any other evidence, for the applying Art. 119) [Yurchenko I.A., 2021: 179]. Prompt application of criminal law to G.'s deviant behavior might have prevented him from committing a more serious crime; he would not have cut off the victim's hand.

One type of cyberstalking is molestation carried out for sexual motives, which is usually termed harassment and is often practiced by supervisors against their subordinates. In Russian criminal law, these acts may be evidence of the crime specified by Art. 133.

Cyberbullying may take the form of public disclosure of personal information often referred to as outing or trickery in English. This involves

revealing personal information, intimate photographs, information about state of health or finances, as well as acts meant to humiliate or blackmail someone such as a former partner, etc. District Court in Ulyanovsk City found a person referred to as N. guilty of posting on internet files entrusted to him by a person referred to as G. These files contained G.'s personal information including personal secrets along with videos and intimate photographs of her. N. had vengeful motives for circulating those materials without G.'s consent because she had broken off relations with him.[25]

A person referred to as A. was convicted of two types of cyberstalking — sexual harassment (harassment in the primary sense) by means of disclosure of personal information (outing and trickery) – under Art. 133(1) and 137(1). While living with his girlfriend, he used a mobile phone and webcam to record images and videos without her consent of their sexual encounters. After their relationship dissolved, he began to blackmail the victim by threatening to circulate the material he had gathered unless she would resume sexual relations with him. As proof that his threat was serious, he posted photos that were in his possession on a social network.[26]

In early 2021 world witnessed internet harassment of US President Donald Trump. The top management of the major social networks in the USA decided that further posting on their platforms in his capacity as president would constitute a risk of violence. After blocking Trump, those services also blocked a large number of his supporters. Twitter, Facebook, Instagram, Reddit, Discord, TikTok, Twitch, Snapchat and YouTube all took part in this unprecedented campaign. Amazon denied hosting on its servers to the Parler network, which was popular with Trump's supporters, and it became inaccessible to users as a result. In response Trump declared, "You can't silence us!" and announced the creation of his own internet platform. The popularity of Telegram soared in this environment to become the second most downloaded app in the United States.

This kind of cyberbullying is considered social isolation or exclusion, i.e., refusal to maintain contact both commercially and informally, which may mean blocking a contact, excluding an instant messenger group, or a gaming community or other community (or communities), etc.

Social isolation of Donald Trump's network brings two problems to the fore. First, there is the question of the legitimacy of censorship and limits

[25] Judicial and regulatory acts of the Russia. Available at: https:// sudact.ru / regular/court/ reshenya-leninskii-raionnyi-sud-g-ulianovska- ulianovskaia-oblast (accessed: 10 February 2021)

[26] Available at: https://pravo.ru/ news /view/118866 (accessed: 10 February 2021)

on freedom of speech. Second, the largest IT corporations are now in fact political powers whose activities demand regulation by law. The resulting conflict has also been seen as evidence of the culture war that has sundered American society.[27]

Yet another type of cyberbullying is an open threat of physical violence, also called a cyberthreat; it consists of a direct or indirect threat to kill someone or inflict bodily harm. In Russian law these acts fall under Art. 119 of the CC RF as death threats or threats to inflict severe injury.

Among the acts classified as internet harassment, there are those that denigrate someone's honor, dignity or business reputation, such as:

blackening a victim's reputation, spreading rumors, or denigration; deliberately presenting them in a negative light by posting photos or videos on the internet (on websites, forums, and newsgroups) or by email. The motive behind these acts may be to disrupt friendly or partnership relations or to take revenge on a former friend;

use of fictional names or impersonation; this includes deliberately impersonating another person by using their password and login to commit antisocial acts, such as insults or humiliation, that will be attributed to the victim.

Ridicule, mockery, provocation or trolling online.

Insults or flaming; this type is characterized by openly making offensive comments, vulgar references and remarks online.

A person referred to as B. was found guilty of ten insults directed at a judge of the Saint Petersburg City Court, obstructing investigation of the case, and inflicting bodily harm on the investigator. The court found that for seven months B. had repeatedly called the judge on a landline telephone and had left various kinds of voicemail including offensive ones. The perpetrator wanted to take revenge on the judge for deciding against her in a civil suit. The investigation classified the matter as commission of ten criminal acts specified by Art. 296(1) of the CC RF and ten more criminal acts specified by Art. 130(1). During the investigation, the public prosecutor dropped the charges under Art. 296(1) because it was found that threats as such were not made, although there was foul language did not have any definite meaning.[28]

[27] Available at: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D0%B8%D1 %80%D0%BE%D0%B2%D0%BA%D0%B0_%D0%94%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%B4%D0%B0_%D0%A2%D1%80%D0%B0%D0%BC%D0%BF%D0%B0_%D0%B2_%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85_%D1%81%D0%B5%D1%82%D1%8F%D1%85 (accessed: 2 February 2021)

[28] (Accessed: 12 February 2021)

Study of the types of cyberbullying outlined shows, first, that there is no single standard in Russian law that prescribes liability for internet harassment. Second, several categories of internet harassment incur administrative liability: insults (Art. 5.61 of the Code of the RF on Administrative Offenses [further COA RF]), assault and battery (Art. 6.1.1 of the COA RF), disorderly conduct (Art. 20.1 of the COA RF). Other types incur criminal liability: assault and battery (Art. 116 of the CC RF), assault and battery by a person subject to administrative penalties (Art. 116.1 of the CC RF), threatening death or infliction of grave injury (Art. 119 of the CC RF), coerced sexual acts (Art. 113 of the CC RF), violation of personal privacy (Art. 137 of the CC RF), breach of the confidentiality of correspondence, telephone conversations, postal, telegraph or other messages (Art. 138 of the CC RF), unlawful access to special technical equipment intended for clandestinely obtaining information (Art. 138.1 of the CC RF), violation of domestic privacy (Art. 139 of the CC RF), extortion (Art. 163 of the CC RF), unlawful access to computerized information (Art. 272 of the CC RF), and the creation, use or distribution of harmful computer programs (Art. 273 of the CC RF).

Finally, several kinds of harassment and internet harassment fall outside the scope of the law, such as periodic telephone calls and SMS texts, surveillance by an obstinate admirer, threats expressed on social networks by fanatics, etc. even though these may be precursors to a grave or extremely grave crime. Then too, some kinds of harassment and internet harassment receive no independent recognition in criminal law. Nevertheless, when they are long-term, systematic and intrusive, they provoke mental anguish that may harm health or lead to suicide.

To address this, some writers suggest following international practice by incorporating a criterion for persecution analogous to foreign ones into the Russian Criminal Code [Barysheva K.A., 2017: 347–350]. For example, §238 of the German Criminal Code prescribes liability for a perpetrator who persistently stalks a person as follows:

Whosoever unlawfully stalks a person by:

seeking proximity to them;

trying to establish contact with them by means of telecommunications or other means of communication or through third persons;

abusing their personal data for the purpose of ordering goods or services for them or causing them to make contact with the perpetrator;

threatening them or a person close to them with loss of life or limb, damage to health or freedom, or

committing similar acts;

thereby seriously infringes their lifestyle shall be liable to imprisonment not exceeding three years or a fine [Golovnenkov P.V., 2021: 346].

Criminal liability becomes more severe in the event that the crime subjects the victim, their relatives or others close to the victim to mortal danger or causes them grave injury or death. The offenses then incur imprisonment for up to ten years.

Complex criteria for stalking are also found in the criminal law of the USA and the United Kingdom.

In 2013 New Zealand passed a law that imposes criminal liability for cyberbullying. A person who is guilty of sending intimidating, racist, sexist or any other message that causes "serious emotional distress" may be punished by imprisonment for two years. In addition, the law distinguishes encouraging suicide as a separate category of crime, which is punishable by imprisonment for up to three years.[29]

Criminal law in other countries designates harassment a crime in the USA and Japan, while revenge porn is a crime in Israel, the USA and the UK, etc.

Introducing liability for harassment (extortion, stalking, bullying, etc.) would, first, not solve the problem of law enforcement and, second, would cause problems in making distinctions between the criteria for crimes that are already present in Art. 110, 110.1, 133, 137 and 138 of the CC RF among others.

It would be more effective to revise the existing criminal law standards in a carefully considered way, and several such proposals have already been made [Yurchenko I.A., 2018: 56].

There is another opinion on this matter. Pavel Golovnenkov in his commentary on §238 of the German Criminal Code notes that several kinds of unlawful persecution by applying psychological pressure to a person (under certain conditions) are punishable under general criteria intended to protect bodily security and personal freedom (for example, personal freedom in §240 of the Code, threats in §241, inflicting bodily harm in §223 and others) and under the provisions of §4 of the Law on Protection of Civil Rights from Acts of Violence and (Unlawful) Harassment (*Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen* [*Gewaltschutzgesetz — GewSchG*] of 11 December 2001, BGBl. 2001 I S. 3513). Law enforcement practice has indicated that, in order to effectively combat infringements of

[29] Available at: http://sanktpeterburg.bezformata.com/listnews/novoj-zelandii-kiberbulling-stal/35038126/ (accessed: 30 January 2021)

personal human rights by lengthy unlawful harassment carried out in a variety of ways, as well as to mitigate the potential for danger that may lie behind such behavior, the Criminal Code had introduced § 238 which sets separate criteria that cover to the fullest extent possible the entire range of criminal acts in the matter (BT-Drs. 16/575, S. 1; 16/1030, S. 1). The benefit that the law protects in this case is the freedom of the individual to exercise their preferences and carry out their personal activities in their own way of life. Furthermore, provisions of §238 (para 2 and 3) protect a potential victim's physical security and life from unlawful harassment (see BT-Drs. 15/5410 S. 6, 16/1030 S. 6) [Golovnenkov P.V., 2021: 347 ff].

Conclusion

The allure of committing crimes via the internet arises from a number of circumstances: the illusion of committing a crime anonymously; the transnational nature of those crimes; the presence of over 4.5 billion persons in cyberspace; the opportunity to commit crimes using artificial intelligence; immediate information exchange; the concealment afforded by the internet for preparation to commit a crime; the uncontrolled financial system, digital accounts and anonymous transactions that can underwrite crimes; and finally the difficulty in detecting and investigating such crimes, which results long-delayed responses. Deviant behavior online is characterized by use of information and communication networks including media and social networks, which is usually accompanied by unlawful access to computer information; the creation, use and dissemination of harmful software; and also improper use of storage, processing or transmission of electronic information and of information and telecommunication networks.

Theft by phishing accounts for over 80% of Russian cybercrime committed by means of modern social engineering technology. Although it runs counter to the recommendations of the Plenum of the Supreme Court of the RF, these crimes are given various interpretations. One way to make law enforcement more consistent is to exclude special categories of fraud from the CC RF and classify such crimes under 158(3)(d) as theft from a bank account or theft of electronic credits under Art. 272, 273 and 274.1.

A common way to seize someone else's property is to use software that makes a system inoperative and demand sending money to a certain account in return for restoring functionality. There is a gap in criminal law's recognition of such acts, and the proposal is to supplement Art. 163(1) to address tries to destroy information.

While media and social networks are regularly used to disseminate fakes, to prevent mass dissemination of fakes that would cause panic and disturb public order, Federal Law of 1 April 2020 No. 100-FZ was adopted to supplement the CC RF with Art. 207.1 "Public dissemination of intentionally falsified information about circumstances that constitute a threat to the life and safety of citizens" and Art. 207.2 "Public dissemination of intentionally falsified information that leads to grave consequences".

Media and social networks have become a platform for inciting, preparing and/or organizing crime or other offenses. The polemics surrounding cyberterrorism were found to be indicative of the debate about increasing liability for use of internet for committing a crime. The position arrived at rejects any agenda to the CC RF. Art. 205(1) stipulates liability for setting off an explosion, arson, etc. as well as for the threat to do so. A threat is a less dangerous action than an actual explosion or arson; if an act of terrorism consists only of the former, then it should incur a punishment toward the minimum provided in Art. 205(1). Hence, disseminating a threat via the internet would not require inclusion in the law as a distinct classification and could be taken into account in applying a sentence within the range of punishments.

Internet harassment is widespread in cyberspace. One type that has not been properly addressed by the law is cyberstalking, which consists of violations of personal privacy (telephone calls, e-mails, surveillance etc.). When they are long-term, systematic and intrusive, they constitute mental harassment that may harm health or lead to suicide, force the victim to alter their accustomed way of living and in some cases are precursors to grave or extremely grave crime. Some legal experts proposed addressing this by inserting a separate article into the CC RF in order to stipulate the liability for cyberstalking. Other writers make the more persuasive case that agenda to the Art. 137 should be made in order to provide the criteria, that would permit making a distinction from the criteria for crimes that are already stipulated by Art. 110, 110.1, 133 and 138 among others.

The state should provide a national corpus of law mandating that internet service providers monitor malicious traffic and block it.

References

Barysheva K.A. (2017) Kiberstalking as a new form of criminal action. In: Ugolovnoe pravo: strategiya razvitiya v XXI veke. Moscow: RG-Press, pp. 347–350 (in Russian)

Bolsunovskaya L. M. (2016) The criminalization of a computer information fraud in the Russian law. *Biblioteka kriminalista*, no 3, pp. 15–20 (in Russian)

Chekunov I.G. (2012) The cybercriminality: term and classification. *Rossijskij sledovatel'*, no 2, pp. 37–44 (in Russian)

Danilov D. (2018) The qualification of Dos-attacks produced by profit interests. *Ugolovnoe pravo*, no 6, pp. 37–42 (in Russian)

Golovnenkov P.V. (2021) The German Criminal Code (Strafgesetzbuch (StGB). Tanslation and comments. Potsdam: University Press, 489 pp. (in Russian)

Inogamova-Hegaj L.V. (2019) The qualification of cybercrimes. In: Ugolovnoe pravo: strategiya razvitiya v XXI veke…. Moscow: RG-Press, pp. 52–55 (in Russian)

Kibal'nik A. (2018) The qualification of a fraud according to recent decision of the Supreme Court of the Russian Federation. *Ugolovnoe pravo*, no 1, pp. 61–67 (in Russian)

Kirilenko V.P., Alekseev G.V. (2020) The garmonization of the Russian anti-criminal legislation with legal standards of the European Council. *Vserossijskij kriminologicheskij zhurnal*, no 6, pp. 898–913 (in Russian)

Klepickij I.A. (2021) New *economic criminal law*. Moscow: Prospekt, p. 984 (in Russian)

Kuleshova G.P., Kapitonova E.A., Romanovskiy G.B. (2020) Legal basis of fight against cyberterrorism in Russia and abroad. *Vserossijskiy kriminologicheskij zhurnal*, no 1, pp. 156–165 (in Russian)

Lopashenko N.A. (2015) Legal reform of a fraud: forced questions and forced answers. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta*, no 3, pp. 504–513 (in Russian)

Russkevich E. (2019) Division of a theft from bank account from adjacent forms of crimes. *Ugolovnoe pravo*, no 2, pp. 59–64 (in Russian)

Solov'ev V.S. (2016) Criminality in social cells of Internet. A study of judicial practice. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta*, no 1, pp. 60–72 (in Russian)

Van der Wagen W., Pieters W. (2015) From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, no 3, pp. 578–595.

Yurchenko I.A. (2021) *The crimes against information security.* Moscow: Prospekt, 208 pp. (in Russian)

Yurchenko I.A. (2018) Stalker as an object of criminal liability. *Vestnik Universiteta O.E. Kutafina*, no 12, pp. 53–56 (in Russian)

Palingenesis of Criminal Law in the Conditions of Digital Reality

Evgeny Russkevich

Associate Professor, Department of Criminal Law, University of the Internal Affairs Ministry, Candidate of Juridical Sciences. Address: 12 Akademika Volgina Str., Moscow 117997, Russia. E-mail: russkevich@mail.ru

Abstract

The article proves that the influence of exponential and combinatorial technological changes has led to a crisis of criminal law, which is expressed in the inability to perform its basic functions due to the permanent and dynamic external environmental impact. The author identifies the following fundamental provisions that should be relied on when making decisions on the modernization of criminal law: the emergence of a new (informational) method of committing a crime does not a priori indicate that it is more dangerous than the traditional one, but in many respects indicates the problem of lag social control from the development of society and changes in crime; the adaptation of the norms of the criminal law to the conditions of the information society should not be associated with the construction of "digital twins" of traditional criminal law prohibitions; the introduction of appropriate amendments to the content of the norms is justified only in cases where the adaptive capacity of criminal legislation to manifestations of digital crime exhausts itself; the recognition of the use of information technologies as a qualifying feature of a crime in general must comply with the criteria for differentiating criminal liability justified in science. The article separately substantiates that the emergence of a "digital personality" will complete the beginning of the transition from the traditional criminal law of the industrial society of the 20th century towards the criminal law of the digital world of the 21th century (criminal law 2.0). First of all, this is due to the fact that artificial intelligence and "digital personality" will fundamentally change the scope of criminal law protection.

Keywords

criminal law, criminal policy, informatization, information technology, information security, computer crimes.

For citation: Russkevich E.A. (2021) Palingenezis of criminal law in the conditions of digital reality. *Legal Issues in the Digital Age,* no 1, pp. 145–159.

DOI: 10.17323/2713-2749.2021.1.145.159

Introduction

Modern criminal law is the result of a longterm development of legal doctrine, legislation and law enforcement. In response to evolutionary changes in social relations, fundamental transformations in the economy, politics and culture, criminal law developed new categories and constructions, leaving behind what had lost its former significance over time. In essence, the development of criminal law has always followed the changing needs of its main object of protection — a human being.

People tend to treat the future as an extension of the present. This type of thinking is based on the idea that the order we have now will continue in the future, albeit in a slightly modified form. A similar logic, of course, is observed in the idea of the development of criminal law.

However, our present, that is experiencing the colossal influence of technological changes, lets us suggest that the future will no longer be its simple continuation. It will be something completely different. At the end of the second decade of the 21th century it is clear like never before that technologies of reverse engineering of the human brain will lead to the creation of Artificial Intelligence and to the emergence of "intelligent machines", as well as to the possible continuation of human life in digital form. These changes will become a point of no return, when our bodies cease to be the center of our identity [Leonhard G., 2018: 69].

The methodological basis of the research is a set of philosophical, general and particular scholar methods. The philosophical and worldview basis of the study is represented by such ideas as the rule of law, the division of law into private and public, etc. The philosophical basis of the study was also formed by the dialectical method of cognition, the use of which made it possible to identify and describe the objective dependence of the transformation of the criminal law mechanism on the impact of digitalization of the sphere of law as a whole.

Concerning the general exploration methods, such as analysis, synthesis, deduction, induction, classification, structural-functional one, etc. were used. Particular importance in the methodology of the study was given to the system method, as well as dialectical materialism.

I. "Crime 2.0" as a consequence of digitalization

"Crime 2.0" is an adaptation of the definition of "Web 2.0" to the problem of crime. Now this term is used by some Western experts to describe

crimes committed with the use of information and communication technologies that have become widespread as a result of the increasing use of the Internet, the rapid development of network and "cloud" technologies, etc. Recently, people have increasingly begun to interact for resolving social and financial issues directly in cyberspace, which has become a place for new crimes against them [Decker C., 2008: 987]. Recently, people have increasingly begun to interact to resolve social and financial issues directly in cyberspace, which has become a place for new crimes against them. Indeed, information technology has become an integral part of our daily life. It is hard t to overestimate the importance of high-tech means of communication in solving global challenges and threats to the modern world. So, stopping SARS has become possible in many ways because of the Internet. A few days after the outbreak of the deadly epidemic, the World Health Organization (WHO) launched a secured site where videoconferences were held on the problem, X-ray images of the lungs were exchanged, on the basis of which a diagnostic protocol was developed along with recommendations for quarantining infected patients. Despite the fact that atypical pneumonia, in terms of the duration of the incubation period, ease of spread and mortality, significantly exceeded the well-known epidemic of the Spanish flu, which carried away in 1918–1920, about 50 million lives [Taubenberger J., 2006], only 8422 persons were affected by it.[1]

At the same time, the rapidly developing architecture of the virtual space not only qualitatively improves our life, but also simultaneously generates new risks and threats. A negative consequence of global digitalization was the emergence of not only a new type of crime (computer crimes), but also a significant change in the nature of crime in general, which, due to the use of information and communication technologies, has acquired previously unusual features.

The performed research allows us to speak about the following six essential features of crimes committed using information and communication technologies:

extraterritoriality — the transnational nature of computer crime is its the most obvious and discussed feature. The global availability of information and communication services means that crime in the information space naturally has an extraterritorial dimension;

virtuality — the information and communication environment is the cornerstone of this crime. By ensuring anonymity and physical distance

[1] World Health Organization. SARS: How a global epidemic was stopped. 2006. Available at: https://apps.who.int/iris/handle/10665/207501 (accessed: 07.11.2020)

from the immediate victim, the virtual space is a significant advantage and, at the same time, a powerful determinant of the commission of a crime. In contrast to the real world, virtuality removes many psychological barriers on the way to the implementation of criminal activity, first of all, those related the maintenance of a feeling (and not always false) of the criminal's personal safety;

hyper-targeting — crimes committed with the use of modern information and communication technologies, perhaps like no others, are characterized by a focus on many victims at once and the ability to cause the chains of multi-level socially dangerous consequences. In case of large viral attacks on the financial sector or on the bank accounts of corporations and citizens, the number of victims can be measured in hundreds or even thousands. For example, a computer attack using the WannaCry ransomware virus began on May 12, 2017 and in a fairly short period of time hit over 500,000 computers in 150 countries. The leaders in the number of infected systems were Russia, Ukraine and India. In this regard, we should refer to the well-known theorem of Stanislav Lem, according to which the destructive power of small groups steadily increases with technological progress. Back in the early 1960s, Lem predicted that in the 21st century, a new industrial revolution will create conditions where not only criminal groups, but also individual criminals will be able to threaten the normal functioning and life of the population of megacities and even states [Lem S., 2012];

multiplicativity — this feature is largely based on such a property of computer crime as the ability to reproduce itself, i.e. multiplicativity. This symptom is most clearly manifested in the distribution of malicious computer programs. A virus attack on a specific organization due to the peculiarities of the architecture of the global information network Internet can result in colossal consequences not only for a single country, but even for a whole group of states. A computer virus, spreading through open communication channels without human participation, will infect all targets available to it, including social security facilities (hospitals, schools, etc.) and government. The other side of this multiplicative property is that the emergence of some form of virtual criminal activity, as a rule, causes new encroachments on information security relations. For example, the emergence of a new computer virus with an atypical way of spreading generates a surge of targeted attacks on protected information resources of both individual citizens and the state;

super-variability — the emergence of a new IT-technology on the mass market of goods or services almost immediately turns into another "re-

set" of crime. Attackers assess innovations as a field of next opportunities for attacking citizens or organizations. Taking into account that technologies are improving rapidly and continuously, it determines that kind of dynamic and permanent process of digital renewal of crime, when some relatively established forms of virtual criminal activity go into oblivion and are replaced by others;

6) systemic latency (hyper-latency) — computer crime is practically not amenable to accurate quantitative measurement. The explanation for this is complex: contradictions in the current regulatory framework, imperfection of law enforcement and statistical accounting mechanisms, massive non-reporting of harm by the victims themselves, as well as the countless and constantly changing nature of "digital crime". In Russia, according to experts, 85–97% of computer crimes are not detected [Agapov P. et al., 2014: 35]. We assume that the real level of latent computer crime in Russia, according to the most conservative estimates, exceeds these figures by several times.

It can be argued that crime that exists in the online space or uses the achievements and capabilities of information technology, manifests itself as a new, poorly studied negative cyber-social phenomenon, which requires a special approach and tools to counteract. Analysis of its characteristics, determination and the development of directions for combating crime 2.0 seems to be the most important task of modern society to ensure national and international security.

II. Digitalization and disruption of traditional criminal law of the industrial society of the 20th century

The traditional mechanism of criminal law protection quite often "does not work" in relation to the changed crime due to the digital transformation that it has undergone.

The most intractable, a kind of systemic challenge for the mechanism of criminal-legal protection of the information society is the previously designated globalism of crimes committed with the use of information technologies. A society in which billions of people are connected by mobile devices that open up unprecedented opportunities in the search, processing and dissemination of information requires a completely different approach both to the legal regulation of these processes and to the protection of the most significant benefits and interests. The extraterritorial nature of Internet communications forces us to admit that no regional and even more so intrastate measures will be sufficient.

We believe that a digital, hyper-connected and hyper-connected world will require a unified international criminal law built on common standards for countering cybercrime. At the same time, the recognition of the jurisdiction of such an "International Criminal Code on Cybercrimes", which establishes a minimum list of encroachments on the security of data and information infrastructure, should be a prerequisite for the participation of every state in all significant international organizations and institutions.

Significant difficulties arise in assessing the encroachments on relations that are emerging in connection with the implementation of human rights in the virtual space. So, for example, is legitimate the question of the possibility of applying the liability for libel to cases of dissemination of deliberately defamatory information about the so-called "digital personality", that is, about the hypertext components of the network image of an individual, formed by him in the online environment for the purpose of self-presentation. Clear, it is possible to speak about the honor and dignity of a "digital personality" only conditionally, implying them only to the real bearer of such qualities — the human person who owns the corresponding "nickname". By spreading deliberately false and defamatory information about the "digital personality", the attacker in one way or another directs these actions against a specific user of this or that Internet resource, that is, commits libel. However, the problem takes on a completely different dimension when the "digital personality" has an artificial origin and belongs to several users at once (for example, it was created and used in a social network for commercial purposes).

In accordance with the criminal law, illegal access to the personal page of another person on a social network can be classified as a crime, but it is very difficult to give a legal assessment of the creation and use of such a page on behalf of another person without his consent. At the same time, such actions can cause significant harm to the rights and legitimate interests of the individual, affect the decision-making on his employment, promotion, etc. Equally, the provisions of modern criminal legislation, as a rule, do not give a clear answer to the question of the qualifications of using technologies for reconstructing another person's face in real time (face swapping technologies). At the same time, such software allows, simply speaking, to "kidnap" the face of another person, to use it for creating certain materials (conditionally compromising or even pornographic).

Another problem is countering encroachments on fundamentally new objects — the so-called "virtual property". One of the most rapidly grow-

ing sectors of the modern economy is the market of multiplayer online games (World of Tanks, Worlds of Warcraft, etc.) and multimedia services (providing films, music, e-books, etc.). At the same time, the virtual space is rapidly commercializing and absorbing more and more cash flows. For real money, users of information services purchase game money, as well as other objects of informational nature that do not have physical (materialized) expression.

Already today there are a lot of special services on the Internet (trading platforms) for the sale of virtual objects used by players in multiplayer online games. It should be noted in Russia the legal nature of this kind of objects has not yet been clearly defined in legal doctrine. Lawyers argue about whether objects such as e-books, iTunes libraries, a social network account or a multiplayer game can be inherited, and whether it is possible to impose an encumbrance on such digital property or use it in enforcement proceedings.

In this regard, the question of the possibile recognizing virtual objects as the subject of theft under criminal law is becoming more and more relevant. "Virtual property" is basically just a computer code. At the same time, unlike other computer data expressing ideas, thoughts, etc., such a code is aimed primarily at imitating objects of the real (physical) world (buildings, vehicles, household items, etc.).

Although such objects exist only on a computer screen, they can be purchased and sold and have a pronounced consumer value. Maintaining the "neutrality" of criminal law regarding the assessment of encroachments on virtual objects is hardly an acceptable approach. The acquisition of real and virtual money, the accumulation of materialized and Internet property have one thing in common — a person's real time spent on this, his labor and, in many cases, real financial resources. In this regard, we can argue that such objects should not and cannot be excluded from legal protection by criminal law only because they have a slightly different nature, are expressed in a different form and look, simply speaking, unfamiliar. Of course, in solving this issue, the doctrine of criminal law largely depends on the development of civil legislation, which, as it seems, should single out such objects as a special category of objects of civil rights, as it's already done, for example, in relation to uncertified securities.

The development of information technologies will lead to significant transformation of transport crime. In these conditions, the doctrine of criminal law receives the need to develop a fundamentally new approach to the legal assessment of accidents involving such vehicles. At the moment, only one thing is clear: the traditional provision on the responsibility of the

driver in such a situation will not work, since he simply does not exist in such a situation.

The mechanism of legal regulation is driven by the state, namely by the activities of its competent authorities. At the same time it should be stated that this element of the mechanism of legal protection is experiencing significant difficulties in countering computer crime. Along with the lack of experts, technical lagging behind and outdated tactics of counteraction, one should also emphasize the unwillingness of police and judicial bodies to see a new digital dimension in the "old" norms of criminal law. In this aspect, one of the main tasks is to overcome the "traditional", i.e. "non-digital" understanding of criminal law by law enforcement officers. This is a rather complex and multifaceted problem that concerns both the initial training of future officers in educational institutions and the advanced training of police personnel in office. At the same time, we can note that the leading role in this regard belongs the doctrine of criminal law, which must first describe, classify and explain the crime of the information society, and thereby ensure the appropriate content of such educational programs.

Problems of procedural implementation of criminal law in the context of crime digitalization are also numerous and complex. At the same time, they are not in themselves the subject of this study. It should only be noted that the doctrine of criminal procedure faces a fundamental research task, without a successful solution of which all achievements of the doctrine of criminal law will be practically useless. As before, these related branches of legal knowledge should develop in concert, keeping up with and reinforcing each other in solving urgent problems of combating crime.

The above described systemic changes in social relations (and not only them) have a disruptive effect on the mechanism of criminal law protection, causing a state of disruption of criminal law — the inability to perform its basic functions due to permanent and dynamic external environmental impact. In the most simplified form, this is expressed in the idea of the complete failure of the criminal law mechanism in the face of the urgent threats of the 21st century and the justification of the need for a completely new model of combating crime.

We can highlight the following fundamental provisions that must be taken into account in the course of future changes in the criminal law:

the emergence of a new cyber method of committing a crime does not mean that it is more dangerous than the traditional one, but in many respects indicates the problem of social control lagging behind the development of society and changes in crime;

the adaptation of the criminal law to the conditions of the information society should not be associated with the construction of "digital twins" of traditional criminal law prohibitions. Such modernization of the criminal legislation will inevitably lead to excessive duplication of its provisions, leading to increasing number of rules competing with each other. In this part, a significant direction in adapting the criminal law mechanism to countering crimes committed with the use of information technology is overcoming the traditional — not digital — perception of criminal law;

amendments to the criminal law norms are only justified in cases where the adaptive capacity of criminal legislation in relation to the new digital crime is exhausted, and the interpretation of these norm goes beyond the meaning of the existing law, filling the systemic semantic gap, which already means the analogy of law;

the recognition of the use of information technologies as a qualifying sign of a crime must comply with the criteria for the differentiation of criminal liability justified in legal doctrine. At the same time, the obligatory grounds for making such a decision are: a) the need to recognize the use of e-technologies as a qualifying sign of a crime is established by the norms of international law and b) the use of information technologies has become widespread in the commission of a crime and has significantly influenced the state of the rights and interests of citizens protected by law.

III. Criminal law of the digital world in the 21th century

The transition to criminal law of a new generation will be associated with a change in our ideas about the key sign of a crime — a socially dangerous act. With the advent of the digital personality, this act will lose its human-centered physical interpretation. It will be possible to speak of an "act" in relation to any manipulation of computer information performed by a "digital personality". This "activity", as a result of which both members of the physical and cyber world may suffer, will become a new digital form of socially dangerous behavior of a criminal.

The development of the whole brain emulation technology will mean the possibility of a completely new form of life, when the very concept of a person is no longer associated with his biological envelope. It is clear that this life in the cloud will require the same criminal legal protection as in the real physical world, since here we will be dealing not just with computer code, but with a person.

As a result, we will have to revise the concept of a victim of a crime and extend the effect of traditional criminal prohibitions (on murder, kidnapping, human trafficking, libel, etc.) to all attacks against the "digital personality". The very moment of the onset of human death will lose its exclusively biological definition and will receive additional content in what we now call the ordinary destruction of computer information. A related problem is the protection of subjects who will possess a human-like consciousness of non-biological origin. Addressing this issue, one of the most famous professional futurists of our time, Google CTO Ray Kurzweil writes: "... today few people worry about the suffering we inflict on computer programs (but we often complain about the pain that computer programs bring us), but if in the future computer software gets the intellectual, emotional and moral qualities of a person, there will be a problem exactly in that regard ...The machine will become indistinguishable from a living person, whom we consider a conscious being, and, therefore, will share all those spiritual values that we associate with consciousness. This is not a humiliation of human dignity, but rather an elevation of our appreciation of (some) machines of the future. It may be necessary to choose a different terminology for these creatures, since they will be completely different machines "[Kurzweil R., 2019: 244, 256].

Already at this stage of technical development, we can talk about the inclusion of intelligent robots in legal relations. One such example is the humanoid robot Sophia, which was activated on April 19, 2015 by Hanson Robotics from Hong Kong. To create a humanoid robot, the technologies of pattern recognition and self-learning were used. During its short "life" the robot Sophia gave many interviews, was on the cover of a fashion magazine and visited many talk shows. In 2017, the robot was granted Saudi Arabian citizenship[2].

The gradual inclusion of the AI in all spheres of human life has led to the emergence of such a concept as "e-person". For the first time, a proposal for the use of this concept was recorded in subparagraph "f" of paragraph 59 of the Resolution of the European Parliament, together with the recommendations of the Commission on Civil Law Regulation in the Field of Robotics of the European Parliament of February 16, 2017 "Civil Law Regulations on Robotics"[3].

[2] Everything you need to know about Sophia, the world's first robot citizen. Available at: https://www.forbes.com/sites/zarastone/2017/11/07/everything-you-need-to-know-about-sophia-the-worlds-first-robot-citizen/?sh=2839a00e46fa (accessed: 14.01.2021)

[3] European Parliament Resolution of 16 February, 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (accessed: 14.01.2021)

Of course, the question of the model of criminal law protection of such "smart machines" entirely depends on the position of all mankind (as we believe, expressed by universal international organizations) regarding their nature and status. It is rather difficult to predict whether such entities will be recognized as equal to humans, that is, a new non-biological form of intelligent life, or whether their position in general will be comparable, for example, with animals, the criminal legal protection of which we implement in the context of protecting public morality.

A mixed scenario is very likely possible, when, depending on the level of reproduction of the intellectual and emotional qualities of a person, such cyber-physical systems will be differentiated in the legal field — as equal to a person, that is, full-fledged participants of social relations, new subjects of law, and as automated systems with limited functions (abilities) of artificial intelligence, that is, as high-tech devices, i.e. things.

A key indicator of the transition to "Criminal Law 2.0" will also be a change in the traditional understanding of the subject and the subjective side of *corpus delicti*. With external autonomy, such machines are and will remain nothing more than tools in the hands of a human. Consequently, either the owner or the developer should be held liable for harm caused by their use. Here the traditional model of the personal responsibility of an individ is triggered, the behavior of which (active or passive) in interaction with a complex technological system was the direct cause of the negative consequences. At the same time, the "digital personality" and artificial intelligence (in any form of their existence) will be independent subjects of law. This means that they should also be recognized as subjects of criminal responsibility. Thus, the theory of criminal law about the subject of a crime will move to a fundamentally new stage of development, when not only an individual and (or) legal entity, but also a digital clone of an individual, as well as AI will be recognized as the subject of crime.

Expanding the conception of the subject of crime will give rise to the problem of revising legal categories such as guilt, motive and purpose of committing a crime. The psychological theory of guilt will remain acceptable only to the physical representatives of Homo Sapiens. For AI and individuals who would continue their life in digital form, it can only be applied using a kind of legal fiction, when we agree that such subjects also have a psyche that allows them to "be aware, foresee and desire." However, as already shown above, this question will first of all need to be raised and resolved in relation to persons who have continued their lives in the digital world.

Conclusion

It is impossible to predict exactly what the future will be like. At the same time, one is clear — technologies will be much deeper and more firmly woven into our daily life. In a hyperconnected world, criminal risks will multiply. For numerous devices and applications that make life much easier, mankind will have to pay with the emergence of "digital crime", which will actively exploit the achievements of the fourth industrial revolution.

The progress in the development of the "Internet of Things" is fascinating. The advent of autonomous vehicles and the concept of a possible future — programmed accident-free and conflict-free road traffic — creates an optimistic view of global security. But at the same time, the potential catastrophic consequences that can occur if someone illegally gains access to such a system and changes its settings for at least a few minutes are quite clearly visible.

The Internet and digital technologies, the "digitalization" of crime are already having an impact on the Russian criminal law. However, we can say for sure — this is just the beginning. The next years will bring much more serious difficulties in the implementation of criminal law protection.

As a global and interconnected world takes shape, individual approaches to countering crime will need to be analyzed and revised. At the same time, it is extremely important that the "digitization" of the Russian criminal law does not lead to the destruction of the essential features of this branch of law. A significant part of adapting the criminal law mechanism to countering cyber crimes, in our opinion, is overcoming the "traditional", "non-digital" perception of criminal law. This is a rather multifaceted problem, which concerns not only the training of personnel in educational institutions and the advanced training of existing law enforcement officers.

The essential features of crimes committed with the use of information technologies are: a) extraterritoriality; b) virtuality; c) hyper targeting; d) multiplicativity; e) supervariability; f) systemic latency (hyperlatency).

Taking into account the rapid digitalization of public relations, we can conclude about the disruptive impact of information and communication technologies on the mechanism of criminal law protection (disruption of criminal law).

The following fundamental provisions can be distinguished, which should be relied upon to overcome this crisis and make a decision on the modernization of the criminal law:

the emergence of a new (informational) method of committing a crime does not a priori indicate that it is more dangerous than the traditional one, but largely indicates the problem of social control lagging behind the development of society and changing crime;

the adaptation of the criminal legal norms to the conditions of the information society should not be associated with the construction of "digital twins" of traditional legal prohibitions. Such modernization of criminal legislation will inevitably lead to excessive duplication of its provisions, expressed in presence of a significant number of norms competing with each other exclusively at the junction of the problem of distinguishing between the virtual and the real in law. In this part, a significant part in adapting the criminal law mechanism to countering cyber crimes is overcoming the traditional — not digital — perception of criminal law;

the adoption of amendments to the criminal law is justified only when the adaptive capacity of criminal legislation to digital crime exhausts itself, and the interpretation of the norm goes beyond the meaning of the law, filling the systemic semantic gap, which in fact is already an analogy of law;

the recognition of the use of information technologies as a qualifying sign of a crime must comply with the criteria for the differentiation of criminal liability justified in legal doctrine. At the same time, the obligatory grounds for making such a decision are: a) the need to recognize the use of e-technologies as a qualifying sign of a crime is established by the norms of international law and b) the use of information technologies has become widespread in the commission of a crime and has significantly influenced the state of the rights and interests of citizens protected by law.

The emergence of the "digital personality" will complete the beginning of the transition from the traditional criminal law of of the 20th century industrial society to the criminal law of the digital world of the 21th century. ("Criminal Law 2.0"). This is primarily due to the fact that AI and "digital personality" will fundamentally change the scope of criminal law protection.

The complexity of digitalization of the criminal law sphere implies an increased responsibility of the academic community, which must provide an appropriate level of understanding of the emerging trends. The attempt made in this article to predict the development of criminal law, of course, does not pretend to be absolute, it is subjective, and therefore probabilistic in its nature. At the same time, there is no doubt that the joint efforts of philosophers, sociologists, high-tech specialists and lawyers will make it

possible to obtain a fairly accurate forecast of the evolution of criminal law in a digital reality.

References

Agapov P., Borisov S. et al. (2014) *Counteraction to cybercrime in the aspect of national security.* Moscow: Academy of the General Prosecutor's Office, 136 p. (in Russian)

Bostrom N. (2007) Technological revolutions and problem of prediction. In: Allhoff F., Lin P., Moor J., Weckert J. (eds.) Nanoethics: the ethical and social implications of nanotechnology. Hoboken (N.J.): Wiley-Interscience, pp. 101–118.

Brenner S. (2012) *Cybercrime and the law: challenges, issues and outcomes.* Boston: Northeastern University press, 263 p.

Decker C. (2008) Cyber-crime 2.0: An argument to update the United States criminal code to reflect the changing nature of cyber-crime. *Southern California Law Review*, no 5, pp. 972–995.

Grabosky P. (2016) *Cybercrime: keynotes in criminology and criminal justice series.* New York: Oxford university press, 168 p.

Kurzweil R. (2019) *Evolution of the mind or the endless possibilities of the human brain based on pattern recognition.* Moscow: Eksmo, 352 p. (in Russian)

Leonhard G. (2018) *Technologies against man*. Moscow: AST, 320 p. (in Russian)

Lem S. (1968) *The sum of technologies.* Moscow: Mir, 1968. 608 p. (in Russian)

Lv A., Luo T. (2018) Authoritarian practices in the digital age. asymmetrical power between internet giants and users in China. *International journal of communication,* no 12, pp. 3877–3895.

Meissner M., Wübekke J. (2016) IT-backed authoritarianism: Information technology enhances central authority and control capacity under Xi Jinping. China's Core Executive, Leadership Styles, Structures and processes under Xi Jinping. *Mercator Institute for China studies,* no 1, pp. 52–57.

Ohlberg M., Ahmed S., Lang B. (2017) Central planning, local experiments: the complex implementation of China's Social Credit System. *Merics China Monitor,* no 43, pp. 1–15.

Qianyun Wang (2016) *A study of cybercrime comparative criminal law: China, US, England, Singapore and the Council of Europe.* Rotterdam: Erasmus University Press, 381 p.

Rhaman M. et al. (2009) Cyberspace claiming new dynamism in the jurisprudential philosophy: a substantive analysis of conceptual and institutional innovation. *International Journal of Law and Management,* no 5, pp. 274–290.

Schwab K. (2018) *The fourth industrial revolution.* Moscow: Eksmo, 288 p. (in Russian)

Sithigh D., Siems M. (2019) The Chinese social credit system: a model for other countries? *EUI Working papers,* no 1, pp. 1–30.

Taubenberger J., Morens D. (2006) 1918 Influenza: The mother of all pandemics. *Rev Biomed*, no 1, pp. 69–79.

Williamson D. (2017) China's online consumerism: managing business, moral panic and regulation. Available at: https://lancaster.academia.edu/DermotWilliamson (accessed: 17.02.2021)

Zhang T. et al. (2015) Using big data theory to establish a new standard for Social Credit System. *Information China*, no 10, pp. 94–95.

Comment

The Right to Access to Privacy of Correspondence and Russian Judicial Practice

Anzhelika Izotova

PhD Student, Law Faculty, National Research University Higher School of Economics. Address: 20 Myasnitsky Str., Moscow 101000, Russian Federation. E-mail: aizotova@hse.ru.

Abstract

Analysis of ways of limiting secrecy of correspondence in Russian judicial practice.

Keywords

e-privacy, privacy of correspondence, secrecy, confidentiality, rights, restriction.

For citation: Izotova A.N. (2021) The Right to Access to Privacy of Correspondence and Russian Judicial Practice. *Legal Issues in the Digital Age*, no 1, pp. 160–168.

DOI: 10.17323/2713-2749.2021.1.160.168

In the past few years, there has been an increase in the number of cases in Russian courts dealing with access to information constituing the secrecy of correspondence. Although judicial practice is not an official source of law in Russia, it plays an important role in identifying and filling gaps in the legal regulation of the processing such information.

A significant step towards expanding the content of secrecy of correspondence was made by the Constitutional Court of Russia. In the case on checking the constitutionality of the provisions of the Federal law "On Communications", it gave a broad interpretation of the constitutional provision on the secrecy of correspondence (part 2 of article 23 of the Constitution of the Russian Federation: Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages),[1] indicating, that information constituting a secret of

[1] Constitution of the Russian Federation. Available at: URL: http://www.kremlin.ru/acts/constitution (accessed: 20.03.2021)

correspondence is any information transmitted and stored by means of communication, including the messages of users and information about such messages (metadata).[2] The position of the Constitutional Court was subsequently used as the basis of court decisions in many other disputes regarding the secrecy of correspondence. Russian legislation imposes the obligation to protect privacy of correspondence on providers[3] — telecom operators, postal operators, organizers of instant messaging services,[4] that is, on persons who have gained access to information constituting a secret of communication by virtue of their professional activities. Among other measures to protect the privacy of correspondence, providers are required to ensure that access to information about messages and its metadata is restricted. The Constitution of Russia establishes the conditions for access to the secrecy of correspondence:[5] 1) only by court decision, 2) in cases provided for by Federal law, 3) only to the extent necessary, 4) in order to protect the foundations of the constitutional order, morality, health, rights and legitimate interests of others, ensuring the defense and state security. The legislation obliges Telecom operators,[6] owners of information resources on the Internet to store information about messages transmitted by their users, as well as these messages themselves, and provide this information to law enforcement agencies, in cases established by laws.[7] Taking this into

[2] Resolution of the Constitutional Court of Russia No. 345-O. October 02, 2003. Available at: URL: https://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-02102003-n-345-o-ob/ (accessed: 20.03.2021)

[3] Article 9 of Federal Law "On Information, Information Technologies and the Protection of Information". July 27, 2006 No. 149-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/24157 (accessed: 20.03.2021); Article 63 of Federal Law "On Communication". July 07, 2003 No. 126-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/19708 (accessed: 20.03.2021); Article 15 of Federal Law "On Postal Communications". June 24, 1999 No. 176-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/14140 (accessed: 20.03.2021)

[4] Instant communications organizer means organizer of information distribution in Internet in case of performance of the activity on the provision of functionality of information systems and/or programs for electronic data processing machines that are aimed at and/or used for electronic communication exclusively between the users of these information systems and/or programs for the electronic data processing machines where the sender of electronic message defines the receiver or receivers of that electronic message, posting in Internet of public information by the users and transfer of electronic messages to the indefinite scope of persons is not stipulated (Article 10.1 of the Federal Law "On Information, Information Technologies and Protection of Information"). Such organizers include for instance messengers.

[5] See Part 2 of Article 23 and Part 3 of Article 55 of the Constitution of the Russian Federation.

[6] See Article 64 of the Federal Law "On Communication"; Article 10.1 of the Federal Law "On Information, Information Technologies and the Protection of Information".

[7] These bodies include Internal Affairs Agencies, Federal Security Service bodies, Federal Government Agency for National Guard, Customs Authorities, External Intelligence

account, as well as the criminal procedure legislation, only law enforcement agencies shall have the right to access the secrecy of communications during investigative actions and only on basis of a court decision.[8]

The provisions of the legislation, including Government decrees,[9] on the storage of information constituting the secrecy of correspondence and on the procedure of interaction between providers and law enforcement agencies, have been relentlessly criticized, since their implementation may be associated with abuse by law enforcement agencies and lead to a violation of the secrecy of correspondence. In particular, it concerned the provisions of the Russian Government Decree No. 538 on the possibility of round-the-clock remote access of the Russian Federal Security Service to the information systems of the Telecom operators. The legality of this provision was the subject of court hearing, and the court rightly recognized the decision as legal, since it only establishes the procedure for interaction between Telecom operators and law enforcement agencies, but does not cancel the need to obtain a court decision to access information constituting a secrecy of correspondence.[10]

Judicial practice shows that, in addition to the criminal prosecution bodies, other state authorities also claim to gain access to the secrecy of correspondence. A number of court cases were aimed to establish legal basis for the right on such an access.

Service, Federal Penitentiary Service (Article 13 of the Federal Law "On Operational Investigative Activities". August 12, 1995 No. 144-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/8220 (accessed: 20.03.2021)

[8] The Russian Federation Code of Criminal Procedure. URL: http://www.kremlin.ru/acts/bank/17643 (Accessed 20.03.2021); Federal Law "On Operational Investigative Activities". August 12, 1995 No. 144-FZ. Availabe at`: URL: http://www.kremlin.ru/acts/bank/8220 (accessed: 20.03.2021)

[9] Decree of the Government of the Russian Federation dated August 27, 2005 No. 538 "On approval of rules of interaction between the communication operators and the authorized public authorities that carry out investigation activities". URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102099619 (Accessed 20.03.2021); Ruling of the Government of the Russian Federation dated July 31, 2014 No. 759 "On rules of storage by the organizers of the information spread in Internet on the facts of acceptance, transfer, delivery and/or processing of voice data, written text, images, sounds or other electronic communication of Internet users and the information on the users, its provision to the authorized public bodies that carry out investigations or secure the safety of the Russian Federation". Available at: URL: http://publication.pravo.gov.ru/Document/View/0001201408060015 (accessed: 20.03.2021)

[10] Appelate Ruling of the Supreme Court of the Russian Federation dated March 05, 2019 No. APL 19–53. Available at: URL:https://legalacts.ru/sud/apelliatsionnoe-opredelenie-apelliatsionnoi-kollegii-verkhovnogo-suda-rf-ot-05032019-n-apl19-53/ (accessed: 20.03.2021)

One of these bodies is the Federal Antimonopoly Service (FAS).

In the dispute between the Telecom operator and the regional FAS Department, the issue of the legality of bringing the Telecom operator to administrative responsibility for failure to comply with the requirements of the antimonopoly authority was considered, namely the refusal to provide information about incoming SMS messages to the phone number specified in the request for a specific date.[11] The position of the FAS was that it has the right to access secrecy of correspondence, since the legislation on advertising[12] imposes on legal entities the obligation to submit to the antimonopoly authority, upon its reasoned request, the necessary information (including information constituting commercial and other secrets protected by law), and also provide authorized officials of the antimonopoly body with access to such information. The courts of first and appellate instances supported the FAS in the dispute. However, the Supreme Court overturned the decisions of the lower courts.[13] The Supreme Court of the Russian Federation took the side of the Telecom operator, which denied the FAS access to the secrecy of correspondence. The court's reasoning was based on the norms of the Law "On Communications", from which it follows that information about subscribers and the communications services provided to them can only be provided to the investigation bodies.[14] Since the FAS does not belong to such bodies, the Supreme Court considered the refusal of the Telecom operator to provide such information to the FAS as lawful.

The same position was expressed by the Supreme Court of Russia in a similar dispute between the territorial Office of the Federal Bailiffs Service and a telecom operator. The courts of the first, appellate and cassation instances took the side of the state body, considering that it had the right to request the necessary information to supervise the return of overdue debt. At the same time, the Supreme Court of the Russian Federation recognized the request of the territorial Office Federal Bailiffs Service to provide the telecom operator with detailed information about telephone conversations on a specific phone number illegal, using the same reasoning as in the pre-

[11] Ruling of FAS of the Republic of Tyva February 06, 2015 on case No. A144-19.8/14. Available at: URL: https://tuva.fas.gov.ru/solution/9463 (accessed: 20.03.2021)

[12] Federal Law "On Advertisement" March 13, 2006 No. 38-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/23532 (accessed: 20.03.2021)

[13] Ruling of the Supreme Court of the Russian Federation March 04, 2016 No. 307-AD15-18844. Available at: URL: https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-04032016-n-307-ad15-18844-po-delu-n-a56-148022015/ (accessed: 20.03.2021)

[14] See Article 53 and 64 of the Federal Law "On Communication".

viously described dispute between the telecom operator and the antimonopoly authority.[15]

Thus, the jurisprudence did not allow an extensive interpretation of the legislation in relation to the access of state bodies to the secrecy of communications.

In addition to the access of third parties to the secrecy of correspondence, the issue of access to the correspondence secrecy of the providers themselves arises in judicial practice. Russian legal doctrine and legislation classify communication secrecy as a professional secret, that is, providers are obliged to ensure the protection of information that they have in connection with the implementation of their professional activities.[16] In particular, the Law "On Communications" stipulates that familiarization with information transmitted over telecommunication networks is possible only by authorized employees of a telecom operator. In other words, only individual employees of a Telecom operator have access to information related to the secrecy of communication in order to fulfill the contract for the provision of communication services.[17]

The legislation does not contain any provisions on providers' access to information constituting a secret of correspondence for purposes other than those mentioned above. The lack of certainty on this issue has led to a number of legal disputes. An example is a dispute between Google LLC and an email user.[18] The e-mail user filed a lawsuit against Google LLC because he found that the advertisements embedded in the text of the letters matched the content of his e-mail. After hearing the dispute, the panel of judges concluded that Google LLC monitored the user's email correspondence for marketing purposes and thereby violated the secrecy of his correspondence. This dispute was the first where the court indicated the inadmissibility of the provider's arbitrary use of the communication secret for their own purposes.

Further jurisprudence gave a broad interpretation of the provisions of the legislation on the access of providers to information constituting the

[15] Ruling of the Supreme Court of the Russian Federation August 29, 2018 and November 14, 2018 No. 308-KG18-8447. Available at: URL: https://legalacts.ru/sud/opredelenie-verkhovnogo-suda-rf-ot-29082018-n-308-kg18-8447-po-delu-n-a53-186852017/ (accessed: 20.03.2021)

[16] See Article 9 of the Federal Law "On Information, Information Technologies and the Protection of Information").

[17] See Clause 3 of Article 63 of the Federal Law "On Communication".

[18] Appellate Ruling of the Moscow City Court September 16, 2015 on case No. 33-30344. Available at: URL: https://sudact.ru/regular/doc/VZjNXeuoUsHr/ (accessed: 15.03.2021)

secret of communication. As a result of this interpretation, one more reason can be distinguished, for the achievement of which providers have the right to independently process information related to the secrecy of correspondence. Such a reason is to provide state bodies, upon their legitimate motivated requests, with information that is not related to the secret of correspondence, but for the establishment of which it is necessary to process the information constituting the secret of correspondence by the provider.

FAS brought the Telecom operator to administrative responsibility for refusing to provide information about a subscriber who, according to FAS, visited a certain web site at a specific time from a specific IP address. The Telecom operator motivated his refusal by the need to interfere with the secrecy of the subscriber's communications to provide the requested information, which is contrary to Art. 23 of the Constitution of Russia limiting the secrecy of communication only on the basis of a court decision. The Supreme Court of Russia sided with the state body and ordered the telecom operator to provide the requested information.[19]

The position of the court was based on the arguments that information about the user of communication services refers to personal data.[20] Also, information about the user of communication services does not belong to the secrecy of correspondence protected by law, since this data was not established in the process of providing communication services. Accordingly, information about a user who accessed the Internet at a specific time with a specific IP address can be provided to government agencies. The processing by the telecom operator of information constituting a secret of correspondence (time of the Internet connection, site address, IP address, etc.) to establish information about the user in this case will not constitute a violation of the secrecy of crrespondence.

Other courts in subsequent disputes followed the position of the Supreme Court expressed in the indicated decision.[21]

---

[19] Ruling of the Supreme Court of the Russian Federation dated March 30, 2016 No. 82-AD16-1. Available at: URL: https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-30032016-n-82-ad16-1/ (accessed: 20.03.2021)

[20] Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ. Available at: URL: http://www.kremlin.ru/acts/bank/24154 (accessed: 20.03.2021); Article 53 of the Federal Law "On Communication".

[21] Ruling of the Eighth Arbitration Appeal Court November 01, 2016 No. A70-4914/2016. Avaulable at: URL: https://kad.arbitr.ru/Document/Pdf/a12e5d2f-9e02-4a98-83d3-fc6558fc-d6f0/%D0%9070-4914-2016__20161101.pdf?isAddStamp=True (accessed: 20.03.2021); Ruling of the Ninth Arbitration Court of Appeal dated November 26, 2019 No. 09AP-57241/2019.

Thus, the analysis of the above judicial practice shows that the operator's actions to process the subscriber's communications in order to fulfill the contract for the provision of communication services, as well as actions to fulfill the obligation to provide state bodies with information that does not in itself relate to the secrecy of correspondence, are considered lawful and do not violate the privacy of subscribers' correspondence.

This conclusion is at odds with the European approach aimed at more serious protection of information constituting a secret of communication, including from the provider itself. European Court of Human Rights (ECHR) in Benedik v. Slovenia[22] assessed the actions of the Internet provider in a similar dispute. The complaint was based on the fact that the Internet provider, in response to a police request, provided information about a user who visited a specific site using a specific dynamic IP address. The ECHR drew attention to the fact that in order to respond to the police request, the Internet provider had to evaluate the stored data related to telecommunications processes. The use of this data is in itself a violation of privacy and requires a court order. Therefore, the ECHR found the actions of the Internet provider in violation of Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[23]

It should be noted that the examples given in Russian judicial practice relate to disputes when the issue concerns solely the provision of information about subscribers to state bodies. If the request contains a requirement to provide information about the subscriber and information about the connections, the courts divide the requirements specified in the request of the state body and recognize the requirements to provide information about the connections (metadata) as illegal.[24]

Not so long ago, the courts issued a number of decisions in cases of challenging the actions of state bodies to hold Telecom operators accountable for refusing to provide details of connections made using a specific

Available at: URL: https://kad.arbitr.ru/Document/Pdf/35e5e7ee-3cb8-48b8-874b-737357f3d2c7/bc3ad46a-883d-4a81-95a1-fd509dfa7165/A40-127165-2019_20191126_Postanovlenie_apelljacionnoj_instancii.pdf?isAddStamp=True (accessed: 20.03.2021)

[22] Ruling of the European Court of Human Rights April 24, 2018 on case of Benedik v. Slovenia (No. 62357/14). Available at: URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-154288%22]} (accessed: 20.03.2021)

[23] European Human Rights Convention. Available at: URL: https://www.echr.coe.int/documents/convention_rus.pdf. (accessed: 20.03.2021)

[24] Ruling by the Supreme Court of the Russian Federation October 11, 2016 No. 82-AD16-5. Available at: URL: https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-11102016-n-82-ad16-5/ (accessed: 20.03.2021)

phone number. Thus, the court of first instance in its decision declared illegal the refusal of the operator to provide the tax authority with information about connections made from a specific phone number.[25] The court concluded that under the secret of telephone conversations is meant any information available to the Telecom operator and concerning a specific subscriber, allowing him to be identified, as well as to establish the content of his communications. In the court's opinion, the fact that the tax authority does not have information about the user of the number in respect of whom information about the connections was requested let us suggest that such information is impersonal and cannot be classified as a secret of communication. This position was supported by higher courts, including the Supreme Court of the Russian Federation.[26]

The conclusions of the courts on this dispute raise a number of questions. A request from the tax authority was sent to obtain information about the connections of a specific telephone number. At the same time, as rightly noted in the legal literature [Savelyev A.I., 2017: 320], a person can be identified by means of various identifiers, including a telephone number. Of course, the state is interested in processing the information accumulated by operators to ensure the implementation of its public functions. However, the use of this kind of information is permissible only under the condition of irreversible loss of connection with a specific person, which in turn needs regulatory legal support [Dvinskikh D.Yu., Talapina I.V., 2019: 17]. Since the tax authority knows the telephone number of the user of communication services, there is no need to talk about the impossibility of identifying the user with communication services. If we recall the position of the courts in the case discussed above with the participation of the FAS, then it will not be difficult for a state body to contact a telecom operator with a request to provide information about the subscriber who made a specific connection, and thereby obtain complete information about the connections of a particular person.

The given example does not allow us to speak about the proper provision of confidentiality of information constituting the secrecy of corre-

[25] Judgment of the Arbitration Court of Moscow City February 06, 2020 on case No. A40-272978/19-140-6979. Available at: URL: https://sudact.ru/arbitral/doc/GJCIOi4Vbn5d/ (accessed: 20.03.2021)

[26] Ruling of the Ninth Arbitration Court of Appeal June 08, 2020 No. 09AP-17966/202, Ruling of the Arbitration Court of Moscow District September 21, 2020 on case No. A40-272978/2019, Ruling of the Supreme Court of the Russian Federation. January 19, 2021 No. 305-ES20-21500. Available at: URL: https://kad.arbitr.ru/Card/7109553c-f3c2-4a7e-a9dd-408bd98be43f (accessed: 20.03.2021)

spondence. Research on privacy in recent years has shown that "depersonalization" by deleting a username does not preclude violation of the privacy of communications. There are a large number of sources, information from which, after combining with anonymous data, allows you to identify a person [Ohm P., 2010].

So, the current judicial practice in matters of access to the secrecy of communication proceeds from the literal interpretation of the law and indicates that law enforcement agencies have the right to access secrecy of correspondence on the basis of a court decision and that other state bodies have no such right.

Concerning the providers' access to the secrecy of correspondence that they have due to their professional activities, the judicial practice is just being formed. Today, an analysis of judicial practice allows us to say that providers have the right to gain access to information constituting a secrecy of correspondence in order to provide communication services, as well as to fulfill legal requirements of state bodies by providing information that is not a secrecy correspondence, but the clarification of which requires the provider's access to the secrecy of correspondence.

References

Dvinskikh D.Yu.,Talapina E.V. (2019) Risks of data turnover development in public administration. *Gosudarstvennoye i municipalnoye upravlenie,* no 3, p. 17 (in Russian)

Ohm P. (2010) Broken promises of privacy: responding to the surprising failure of anonymization. Available at: URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (accessed: 20.03.2021)

Savelyev A.I. (2017) Scholar and practical article-by-article commentary to the Federal law "On personal data". Moscow: Statut, 320 p. (in Russian)

Book Review

Intermediary Liability

Ruslan Nurullaev

Senior Lecturer, National Research University Higher School of Economics. Address: 20 Myasnitskaya Str., Moscow 101000, Russian Federation. E-mail: rusnur@gmail.com

Abstract

Book review: Giancarlo Frosio (Ed.). Oxford Handbook of Online Intermediary Liability. Oxford: OUP, 2020, 800 p.

DOI: 10.17323/2713-2749.2021.1.169.178

The influence of online service providers (OSPs) on our lives is ever increasing. Their services are used by billions of human persons.[1] Among ten largest companies in the world by market capitalisation, seven focus their business on providing online services.[2] OSPs affect the outcome of elections[3] and even become a subject of international politics themselves[4]. If anything, the COVID-19 pandemic has further boosted an expansion of online services.[5]

Despite the rising importance of OSPs, we are still far from reaching a consensus on how OSPs should be regulated and when they should be held liable for infringements committed with the use of their services. In different parts of the world actions are taken to increase responsibility of OSPs

[1] Global social media Stats. Available at: https://datareportal.com/social-media-users (accessed: 01.03.2021)

[2] The 100 largest companies in the world by market capitalization in 2020. Available at: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/ (accessed: 01.03.2021)

[3] Social Media Could Determine The Outcome of the 2020 Election. Available at: https://www.forbes.com/sites/petersuciu/2020/10/26/social-media-could-determine-the-outcome-of-the-2020-election/?sh=f3b7a0c26f60 (accessed: 01.03.2021)

[4] After Trump's TikTok Ban, China Readies Blacklist of Foreign Companies. Available at: https://www.nytimes.com/2020/09/19/technology/china-tiktok-wechat-blacklist.html (accessed: 01.03.2021)

[5] E-commerce in the time of COVID-19. Available at: http://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/ (accessed: 01.03.2021)

for the content disseminated with the use of their services.[6] Yet even OSPs recognise that this may be a dangerous path.[7]

Oxford Handbook of Online Intermediary Liability edited by Giancarlo Frosio[8] is written by an international team of authors from different universities and research centres and presents an extensive and multifaceted analysis of the main topics of OSPs' liability. The Handbook promises to "provide a comprehensive, authoritative, and 'state-of-the-art' discussion of intermediary liability by bringing together multiple scholarly perspectives and promoting a global discourse through cross-jurisdictional parallels". It fully delivers on this promise and is essential reading for anyone interested in regulation of online intermediaries.

The Handbook contains 39 chapters collected into 7 logical parts.

Part I features an introductory chapter by Giancarlo Frosio. The chapter provides helpful guidance for the whole Handbook. It explains the Handbook's structure and sets out the most important findings of the chapters coalescing them into a consistent narrative.

Part II (Chapters 2 to 7) lays down a theoretical basis for the rest of the Handbook.

In Chapter 2, Graeme Dinwoodie[9] investigates the definition of "internet intermediaries", its relationship with alternative terms and the taxonomy of internet intermediaries. Dinwoodie suggests that the term "internet intermediaries" should be given a broad interpretation but this should not stop us from attempting "to classify and differentiate among the different actors who are encompassed by the term".

A theoretical framework for OSP liability focusing on monetary and non-monetary liability, as well as primary and secondary liability is pro-

[6] For example, in the EU, the DSM Directive (Directive (EU) 2019/790) adopted 17 April 2019 requires online content-sharing service providers to take additional steps ensuring unavailability of copyright-infringing content. In the US, on 28 May 2020 the President signed Executive Order 13925 which purports to limit immunity of OSPs for the content disseminated on their platforms.

[7] Twitter boss: Trump ban is 'right' but 'dangerous'". Available at: https://www.bbc.com/news/technology-55657417 (accessed: 01.03.2021)

[8] An Associate Professor at the Center for International Intellectual Property Studies at Strasbourg University, a Fellow at Stanford Law School Center for Internet and Society, and Faculty Associate of the NEXA Center in Turin.

[9] Graeme Dinwoodie is the Global Professor of Intellectual Property Law at Chicago-Kent College of Law.

posed by Jaani Riordan[10] in the next chapter. Riordan also looks into theoretical justifications for intermediary liability observing that even in the absence of liability the conduct of OSPs may be important because of its self-regulatory nature.

Martin Husovec[11] in Chapter 4 focuses on the consequences of imposing different species of liability upon internet intermediaries and examines: (1) the scope of damages; (2) their aggregation; (3) the scope and goal of injunctions against OSPs and (4) their associated costs. Husovec persuasively argues in favour of employing a consequences-based approach towards intermediary liability.

Kristofer Erickson[12] and Martin Kretschmer[13] review empirical studies on copyright intermediary liability published during the period from 1998 to 2018 identifying the gaps and limitations of the available empirical research (Chapter 5). They conclude that the flaws of the current safe harbour regime of OSP liability are significant but can be overcome 'through tweaking, rather than overhauling'.

Mariarosaria Taddeo[14] in Chapter 6 expands the analysis of OSP liability by discussing the moral responsibilities of OSPs in relation to managing access to information and human rights, as well as the role and the nature of OSPs' responsibilities in mature information societies.

In the next chapter, Christophe Geiger, Giancarlo Frosio, and Elena Izyumenko[15] look at intermediary liability through the lens of human rights and analyse the impact of intermediary liability on users' rights, OSPs' rights and rights of IP owners. The chapter authors conclude that courts have often used case-by-case analysis to find a balance between competing fundamental rights and that this flexibility should be preserved.

In Part III (Chapters 8 to 15), the authors present an overview of intermediary liability and safe harbours across multiple jurisdictions, focusing on inconsistencies and fragmentation of regulation in each jurisdiction.

---

[10] A barrister at 8 New Square, London.

[11] Assistant Professor of Law at The London School of Economics and Political Science (LSE) and Affiliate Scholar at Stanford Law School Center for Internet and Society.

[12] Associate Professor in Media and Communication at the University of Leeds.

[13] Professor of Intellectual Property Law at the School of Law, University of Glasgow and Director of CREATe, the UK Copyright and Creative Economy Centre.

[14] A Researcher Fellow at the Oxford Internet Institute and Deputy Director of the Digital Ethics Lab.

[15] Lawyer at European Court of Human Rights.

In Chapter 8, Eric Goldman[16] turns to regulation of intermediary liability under US law and reviews 47 USC § 230, a long-standing section regulating immunity of online services under US law, and compares it to some of its foreign counterparts.

In the following chapter, Juan Carlos Lara Gálvez[17] and Alan M. Sears[18] continue with the analysis of intermediary liability rules in Latin America, where development of OSP liability was affected by free trade agreements with the United States.

Luiz Fernando Marrey Moncau[19] and Diego Werneck Arguelhes[20] review the Marco Civil da Internet (Law 12.965/2014), the landmark legislation on OSP liability in Brazil, including the history its adoption and the practice of its application revealing the contrast of the formal legal provisions and the 'law in action' (Chapter 10).

Nicolo Zingales[21] follows up, in Chapter 11, with the overview of intermediary liability in African countries revealing a trend of progressive erosion of intermediary liability protections and increasing pressure on intermediaries to fulfil broad and open-ended public policy mandates.

After that, in Chapter 12, Kylie Pappalardo[22] and Nicolas Suzor[23] explore the principles of intermediary liability in Australia in defamation, vilification, copyright, and content regulation. Pappalardo and Suzor conclude that rules governing intermediary liability in Australia lack coherency and at times do not allow to predict when, exactly an online intermediary will be liable for the actions of third parties.

---

[16] A Professor of Law at Santa Clara University School of Law, where he is also Director of the school's High Tech Law Institute.

[17] The Research and Public Policy Director at Derechos Digitales - América Latina, based in Santiago de Chile.

[18] A Researcher and Lecturer at Leiden University's eLaw Centre for Law and Digital Technologies.

[19] A Non-Residential Fellow at the Stanford Center for Internet and Society and a PhD from Pontif ócia Universidade Catylica of Rio de Janeiro.

[20] Associate Professor of Law at Insper Institute for Education and Research, São Paulo, Brazil.

[21] Professor of Information Law and Regulation at Fundação Getulio Vargas (FGV) Law School, an Affiliate Scholar at Stanford Center for Internet and Society, and a Research Associate at the Tilburg Institute for Law, Technology and Society and the Tilburg Law and Economics Centre.

[22] A Senior Lecturer in the Law School at the Queensland University of Technology (QUT) in Brisbane.

[23] A Professor in the Law School at Queensland University of Technology in Brisbane.

Turning now to Asian countries, in Chapter 13, Kyung-Sin Park[24] reviews intermediary liability in China, India, Japan, South Korea, Indonesia, and Malaysia. Park compares the regulation in these countries with the 'safe harbour' approach used in the EU and US.

In Chapter 14, Danny Friedmann[25] discusses intermediary liability for trade mark and copyright infringement in China. Friedmann argues that due to the advancement of artificial intelligence, the filtering standard for OSPs in China will continue to intensify and OSPs will have to proactively monitor and remove infringing content.

Maria Lillà Montagnani,[26] in Chapter 15, analyses the Digital Single Market Strategy[27] and argues that it introduces an 'enhanced liability regime', a new set of obligations and duties of care changing the 'conditional' nature of intermediary liability in the EU into 'organisational'.

Part IV (Chapters 16 to 26) provides an overview of intermediary liability in specific legal areas, including copyright, trade mark, unfair competition, and privacy infringement. Christina Angelopoulos[28] highlights the lack of harmonisation in EU rules governing intermediary liability and proposes a negligence-based system to fill in this lacuna (Chapter 16).

In the next chapter, Eleonora Rosati[29] analyses direct liability of intermediaries and the right of communication to the public. Rosati discusses case law of the CJEU, focusing on its judgment in *Stichting Brein*[30], a seminal case in which the CJEU considered when an operator of an online platform communicates a work to the public.

Jack Lerner[31] provides detailed overview of secondary copyright infringement liability in the US taking into account the case law and legislative proposals in this area (Chapter 18). Lerner anticipates changes to

[24] A Professor at Korea University Law School.

[25] Assistant Professor of Law, Peking University School of Transnational Law in Shenzhen.

[26] An Associate Professor of Commercial Law at Bocconi University in Milan.

[27] European Commission Communication. A Digital Single Market Strategy for Europe (2015) COM (2015) 192 final.

[28] Lecturer in Intellectual Property Law at the University of Cambridge and a member of the Centre for Intellectual Property and Information Law (CIPIL).

[29] An Associate Professor in Intellectual Property Law at Stockholm University and an Counsel at Bird & Bird.

[30] Stichting Brein v Ziggo BV and XS4All Internet BV [2017] ECLI:EU:C:2017:456.

[31] A Clinical Professor of Law at the University of California, Irvine School of Law and Director of the UCI Intellectual Property, Arts, and Technology Clinic.

the regulation of intermediary liability in the US after the EU's approval of Article 17 of the DSM Directive[32].

Moving on to trade marks, Frederick Mostert[33] highlights the lack of uniform international guidelines for tackling counterfeits problem on the internet and suggests three common principles that can be used as a basis for transnational approach to intermediary trade mark liability (Chapter 19).

In the following chapter, Martin Senftleben[34] discusses development of intermediary trade mark liability in the EU. Senftleben contrasts the approach to trade mark liability with liability for copyright infringement and argues that the increased reliance on algorithmic content identification and filtering systems in trade mark cases may bring undesirable results.

Richard Arnold[35] reviews UK case law on intermediary trade mark liability with a particular focus on injunctions against OSPs whose services are used to infringe rights in trade marks (Chapter 21).

Proceeding to liability outside of intellectual property rights, in the next chapter, Reto M. Hilty[36] and Valentina Moscon[37] discuss intermediary liability in the areas of unfair commercial practices and trade secrets.

In Chapter 23, Emily Laidlaw[38] presents a new 'notice-and-notice-plus' model of intermediary liability for defamation. Laidlaw also explores the possibility of application of this model to other types of harmful speech. The proposed 'notice-and-notice-plus' model can provide more nuanced and well-balanced approach to OSP liability in certain areas, without requiring intermediaries to make legal judgment on user content.

In the next chapter, Tarlach McGonagle[39] reviews the case law of the European Court of Human Rights (including the judgment in *Delfi*[40]) and EU legislation in the area of freedom of expression and intermediary liability.

---

[32] Directive (EU) 2019/790.

[33] Professor of Intellectual Property at the Dickson Poon School of Law, King's College and Research Fellow at the Oxford Intellectual Property Research Centre.

[34] A Professor of Intellectual Property Law, Institute for Information Law, University of Amsterdam.

[35] Judge of the Court of Appeal of England and Wales.

[36] Managing Director at the Max Planck Institute for Innovation and Competition in Munich and Full Professor (ad personam) at the University of Zurich.

[37] Senior Research Fellow in Intellectual Property and Competition Law at the Max Planck Institute for Innovation and Competition.

[38] Associate Professor, Faculty of Law, University of Calgary.

[39] A Senior Lecturer/Researcher at IViR, University of Amsterdam and Professor of Media Law & Information Society at Leiden Law School.

[40] Delfi AS v Estonia [GC] App. no. 64569/09 (ECtHR, 16 June 2015).

Two manifestations of the right to be forgotten in the EU are analysed by Miquel Peguera[41] in Chapter 25: (1) the right to be delisted from search results provided by internet search engines and (2) the right to request removal or anonymisation of personal information by primary publishers.

Eduardo Bertoni[42] continues the discussion of the right to be forgotten in Latin America and concludes that in the absence of judicial decision it may be difficult to require OSPs to delist content (Chapter 26).

Part V (Chapters 27 to 30) discusses online enforcement of intermediary liability and focuses on monitoring and filtering obligations, website blocking, and enforcement by administrative bodies.

In Chapter 27, Aleksandra Kuczerawy identifies and discusses different mechanisms aimed at removal of infringing content from the internet upon request of right holders. Kuczerawy examines 'notice and takedown' (NTD), 'notice and notice' (NN), and 'notice and stay down' (NSD) and assesses the impact of each mechanism on the freedom of expression.

In the next chapter, Giancarlo Frosio and Sunimal Mendis[43] explore the gradual shift from the intermediary liability system based on the principles of negligence and prohibition of monitoring obligation to a system in which some OSPs are required to undertake proactive monitoring and filtering of content. Frosio and Mendis argue that this development may limit the effect of copyright exceptions and limitations and even curtail the use of certain public domain content.

Christophe Geiger and Elena Izyumenko discuss website blocking in Chapter 29. Geiger and Izyumenko review the jurisprudence of the European Court of Human Rights and the CJEU and suggest several criteria that can help to ensure compliance of website blocking orders with fundamental human rights.

In many countries administrative bodies play an important role in policing infringing content online. The practice of intermediary liability enforcement by administrative bodies across several European jurisdictions is investigated in Chapter 30. Alessandro Cogo[44] and Marco

[41] An Associate Professor of Law at the Universitat Oberta de Catalunya (UOC) in Barcelona and Affiliate Scholar, Stanford Center for Internet and Society.

[42] Representative of the Regional Office for South America of the Inter American Institute of Human Rights, Director of the Post-graduated Program on Data Protection at Buenos Aires University School of Law, and Global Clinical Professor at New York University School of Law.

[43] Assistant Professor in Intellectual Property Law at Tilburg University.

[44] Associate Professor at the University of Turin Law School and Director of the Master of Laws in Intellectual Property jointly organized by the World Intellectual Property Organization and the Turin University.

Ricolfi[45] pay special attention to the activities of the Italian Authority for Communication Guarantees (AGCOM), which is authorised to order removal and blocking of infringing content.

Part VI (Chapters 31 to 35) is focused on voluntary measures taken by online intermediaries to police infringing content. This emerging trend transforms the discussion of 'intermediary liability' into that of 'intermediary responsibility' and 'intermediary accountability'.

Chapter 31 identifies and reviews different forms of 'responsible' behaviour beyond the law, such as graduated response, demotion of search results, payment blockades, private DNS content regulation, standardisation of OSPs' obligations, codes of conduct, filtering, and website-blocking. Giancarlo Frosio and Martin Husovec also consider the risks and challenges associated with the increased use of such voluntary measures and private ordering.

In the following chapter, Annemarie Bridy[46] focuses on intellectual property enforcement in the DNS and domain blocking. Bridy pays particular attention to 'trusted notifier' agreements between intellectual property right holders and TLD registry operators, such agreements facilitate online enforcement of copyright by suspending, terminating, or locking domains.

Sergei Hovyadinov[47] in Chapter 32 presents detailed overview of the evolution of intermediary liability in Russia since 2011-12. Hovyadinov focuses on two areas: 'content' – the types of information the government seeks to restrict online, and 'surveillance' – state collection of user data and information about online activities.

Chapter 33 discusses content moderation by online intermediaries and the challenges it presents to the rule of law. Niva Elkin-Koren[48] and Maayan Perel[49] also describe barriers to accountability of online intermediaries and propose a strategy that can overcome such barriers – a reverse-engineering methodology which the authors named 'black box tinkering'.

---

[45] Professor of Intellectual Property at the Turin Law School, Partner at the law firm Tosetto, Weigmann e Associati, and Co-director of the Nexa Center on Internet and Society of the Turin Polytechnic.

[46] An Affiliate Scholar at the Stanford Law School Center for Internet and Society (CIS), and an Affiliated Fellow at the Yale Law School Information Society Project (ISP).

[47] A JSD candidate at Stanford Law School.

[48] A Professor of Law at the University of Haifa, Faculty of Law and a Faculty Associate at the Berkman Klein Center at Harvard University, the Founding Director of the Haifa Center for Law & Technology (HCLT), and a Co-director of the Center for Cyber, Law and Policy.

[49] An Assistant Professor in Intellectual Property Law at the Netanya Academic College in Israel and a Senior Research Fellow at the Cyber Center for Law & Policy, University of Haifa.

Online intermediaries often employ algorithms to police infringing content. In Chapter 34, Ben Wagner[50] examines the meaning of algorithmic accountability, 'the process in which both information systems themselves, their developers, and the organizations behind them are held accountable for the decisions made by those information systems'[51], and the challenges that must be overcome to implement algorithmic accountability.

Part VII (Chapters 36 to 38) discusses international private law issues and extraterritorial enforcement against OSPs. In Chapter 36, Dan Jerker B. Svantesson[52] discusses three examples in which the issue of jurisdiction becomes a major concern for online intermediaries: (1) law applicable to the terms of service used by online intermediaries; (2) requests of law enforcement agencies for provision of user data; and (3) geographical scope of the OSPs' obligations to remove, block, take down, delist, de-index, or de-reference content.

In the next chapter, Michael Geist[53] examines *Equustek Solutions v Google*[54], a recent case in which the Supreme Court of Canada had to decide whether Google can be required to remove search results on a global basis where infringement of intellectual property rights is concerned. Geist comes to a logical conclusion that 'extraterritorial application of court decisions such as those involving Google is that it encourages disregard for the rule of law online, placing internet companies in the unenviable position of choosing the laws and court orders they wish to follow'.

In Chapter 38, Bertrand De La Chapelle[55] and Paul Fehlinger[56] discuss how to move on from the current 'legal arms race' to transnational cooperation of all stakeholders when determining jurisdiction applicable to online intermediaries.

---

[50] An Assistant Professor at the Faculty of Technology, Policy and Management at TU Delft.

[51] See Richard Mason and Ian Mitroff. A Program for Research on Management Information Systems.Management Science, 1973, no 19, p. 475 cited on p. 679 of the Handbook.

[52] A Professor at the Faculty of Law at Bond University, a Visiting Professor at the Faculty of Law, Masaryk University, and a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University.

[53] A Professor of Law at the University of Ottawa where he holds the Canada Research Chair in Internet and E-commerce Law and is a member of the Centre for Law, Technology and Society.

[54] [2015] BCCA 265 (Can.).

[55] The Executive Director and Co-founder of the global multistakeholder organization Internet & Jurisdiction Policy Network.

[56] The Deputy Executive Director and Co-founder of the multistakeholder organization Internet & Jurisdiction Policy Network.

The Handbook presents the results of research of a diverse international team of experts. It addresses all major themes of intermediary liability and investigates law and practice of a large number of jurisdictions revealing the current trends in development of OSP liability. Perhaps the greatest achievement of the Handbook is that it brings together different aspects of intermediary liability into a holistic and logical narrative.

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through, efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among, academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

Legal Issues in the **DIGITAL AGE**

Authors guidelines

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length
Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title
The title should be concise and informative.

Author Details
The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract
The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords
Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References
The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes
The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.

Выпускающий редактор *В.С. Беззубцев*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*

Подписано в печать 30.04.2021. Формат 70×100/16
Усл. печ. л. 11,6.