Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

4/2021

ISSUED QUARTERLY

Articles

Comment

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

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4.

Articles

Research article
UDC: 340
DOI: 10.17323/2713-2749.2021.4.3.33

Personal Legal Status in Context of Technology-Driven Social Experiment

Maria Evgenievna Cheremisinova
Institute of Law and Comparative Legal Studies under the Government of Russian Federation, Moscow, Russia, mech.july@yandex.ru

Abstract

Based on the study of relevant research findings, law enforcement practices and content analysis, the paper identifies the peculiarities of social and legal environment reflecting the experimental nature of life of a modern society. The mutual effects of technologies, social relationships and legal regulations are discussed. It is stated that technologies which initially had an uncertain impact (social, economic, political and legal) have set an evolutionary development trend of modern societies worldwide, only to justify the insight into evolving conditions in which the personal legal status is implemented. In identifying the nature of technological revolution at the current stage, a conclusion is made on the implementation of a vast majority of social relationships in context of technology-driven social experiment. The legal features of this experiment making it different from the previous stages of the technological progress are identified, and the importance of convergence of the community and digital technologies to set directions for development of the law is underlined. Special attention is paid to the category of the personal legal status and aspects of its protection. The factors of its transformation in the given context are studied and the impact of the experiment's legal features on the personal legal status is demonstrated. The paper is aimed at proposing solutions to the issue of preserving legal status of a person as a legitimate party to social and technological processes protected from technocratic manifestations, endowed with the right of choice and opportunities to exercise it. In terms of methodology, the study is based on both general and particular research methods. The former include structured and historical methods while the latter — formal legal method and logical cognitive tools such as analysis, synthesis, induction, deduction. It is proposed to expand the field of application of legal experiment to keep pace with the social relationships dynamics in the context of technological change, help maintain the guarantees

related to the established rights and liberties and also contribute to the development of well-balanced legal controls.

Keywords

personal legal status; technology-driven social experiment; legal experiment; interaction of law and technology; protection of individual rights in a digital age.

For citation: Cheremisinova M.E. Personal Legal Status in Context of Technology-Driven Experiment. *Legal Issues in the Digital Age.* 2021, no. 4, pp. 3–33. DOI: 10.17323/2713-2749.2021.4.3.33.

Introduction

With the rapid pace of technological change social sciences and practices are increasingly faced with new problems. A powerful social impact of the advanced technologies on communities, public law and state is now clearly visible. At this stage the most active processes are those of digitization which are primarily related to the expansion of Internet as a worldwide communication and information network which has been already recognized as a social good[1].

Interestingly, in its early days the Internet was viewed more narrowly as the means of communication and information, with social implications of its expanded use being unclear. However, as technologies evolved to make the Internet a space for the exercise of all fundamental rights and liberties, and as the ambiguous results of its use were assessed, the political, psychological, economic and legal roles of the Web in social and public processes including the formation of personal legal status have become evident.

The Internet's development and expansion has not only shown that modern society worldwide is open to technical innovations without asking their developers and inventors for guarantees and clear explanations of the operating principles. The convenience of use, new exciting services, innovations and economic benefits have largely overweighed the risks users assume while familiarizing themselves with the worldwide web. Meanwhile,

[1] The Internet was recognized as a public good in 2011. The right to access was established by a UN declaration as a fundamental human right and a "social good". Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 16.05. 2011. Available at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf) (accessed: 24.05.2020)

these risks have turned out to be quite serious, with some spilling over into the legal field with its related institutions and mechanisms for protection of rights and liberties. The development of web technologies has set a new trend based on the system of so-called venture capital driven startups which assumes fast deployment and as fast economic return. In other words, innovations now instantly "gain ground", with the economic and social feasibility of further development of services, platforms and devices determined by users [Chugreev V.L., 2015][2]. As evidenced by the adoption of strategic, conceptual and policy documents, governments are making a major focus on such a system to improve their ability to compete[3].

Some authors believe that "due to the openness of modern technology, the spread of related risks and probable threats will only become possible, once it has been deployed, something that cannot be predicted as society itself is becoming a laboratory, and, unlike previously, the nature of technological development is now such that an experiment cannot be separated from use" [Bechmann G., 2012]. This observation does not only confirm close interaction and interdependence between society and technology at the current stage of evolutionary change but also outlines the conditions underlying social relationships and, thus, regulatory development. It is worth noting that the above quote is borrowed from a publication dating back to 2012. Over 10 years elapsed since then technologies have advanced exponentially, only to become part of all life spheres. The world is now at the convergence point, with technologies to include, apart from information and telecommunications, bio, nano and cognitive technologies.

Philosophical works are now concerned with the problem of forming legal consciousness and identifying new civilization development strategies, impact of the technological and cultural change on law, outcomes of human genome studies, new human improvement technologies, legal

[2] In the technological community there is a concept of "technical debt" to identify tasks put aside for the sake of rapid development of a new software. In many cases it means that developers will have to correct and adapt the software code.

[3] See, for example: Russia: Presidential Decree No. 203 of 9 May 2017 "On the Development Strategy of Information Society in Russia in 2017–2030"; Russian Government Resolution No. 313 of 15 April 2014 "On the Approval of the Information Society State Program", National Action Plan to ensure recovery of employment and incomes of the population, economic growth and long-term structural changes in the economy (approved by the Russian Government on 23 September 2020, protocol No. 36, section VII); France: Law No. 2016–1321 of 7 October 2016 on the digital republic (government) (LOI n° 2016–1321 du 7 octobre 2016 pour une République numérique. Available at: https://www.legifrance.gouv.fr (accessed: 24.05.2020); international: Okinawa Charter on Global Information Society (Okinawa, 22 June 2000).

status of cybernetic and genetically modified organisms, and artificial intelligence [Khabrieva T.Ya., Chernogor N.N., 2020]. But the assessment of implications of these processes only recently believed to be science fiction remains exclusively the focus of social sciences. Meanwhile, technologies are developing, as it were, on their own without regard for the social outcomes and "social compatibility" understood, in particular, to be the observance of human and civil rights combined with physical protection.

There is an interesting case of how inventors of nanotechnologies perceive their innovations. Thus, Eric Drexler, pioneer in this domain, has suggested to keep these technologies secret for fear of their potential threat. However, Drexler soon realized that, once he had conceived the idea of nanotechnologies, others could do the same. (In fact, as he later learned, Richard Feynman had already established the main principles in this sphere decades before). Thus, Drexler decided that the only responsible approach would be constructive control of non-reversible development of nanotechnologies [Reynolds G.H., 2003: 179–209].

As regards biotechnologies, it is stated that their unprecedented progress in the second half of the 20th century (human genome deciphering, dissemination of auxiliary reproductive technologies, organ and tissue transplanting, 3D-printing of tissues and organs, cloning, genetic testing and diagnosis, exo-skeletons etc.) has started the so-called biomedicalization of society. Moreover, the ambivalent nature of biotechnologies means that their progress brings about as many opportunities for dramatic improvement of living standards of people as there are threats caused by their tremendous potential effects on human nature [Tsomartova F.V., 2021: 9–10].

Regarding the development and deployment of artificial intelligence (AI), Max Tegmark, professor of physics at the MIT, initiator and president of two civil society institutions, Institute of Fundamental Problems and Future of Life Institute[4] — has confirmed in an interview that developers of complex modern technological systems did not fully understood them. He said "unfortunately, if we are really successful in developing general AI, we will do so without understanding how it works. The alternative approach — no black boxes. Only IAI (intelligent AI approach to building AI we understand)[5]".

The above technologies which owe much of their advance to digitization and informatization have their main peculiarity in that they are fraught

[4] Available at: URL: https://www.livelib.ru/author/872945-maks-tegmark (accessed: 12.01.2020)

[5] Max Tegmark interview. Available at: https://www.youtube.com/watch?v=RL4j4KPwNGM&t=2s (accessed: 16.12.2019)

with the risk of causing unfavourable social implications which are hard (or maybe impossible) to predict [Boroon L., Abedin B., Erfani E., 2021]. Examples of such implications have a delayed effect and are already reflected in law enforcement practices. As they build up, technologies of social life come under legal scrutiny, and a need to define legal aspects of technologies comes to the fore [Tikhonova S.V., 2017: 275–278]; [Spitsin I.N., 2021]. In particular, difficulties in managing personal data in the Internet did not spring up instantly, with modern legal mechanisms protecting data rights emerging as a result of the conflicts handled by courts including the supreme and supranational courts [Lazarev V.V., Gadzhiev Kh. I., 2020].

The Internet developers currently recognize a lack of data management and control in key web protocols as their "technical debt"[6]. However, a wide use of big data processing is now a reality, with information recognized a new economic asset along with hydrocarbons and determining the digital economic development across the board. Also, there is a problem of digital trace which needs to be studied from a perspective of respect for fundamental rights and liberties etc.

Thus, it could be asserted that the technology with initially uncertain social, economic, political and legal impact has globally set an evolutionary vector of development of modern society.

It is this feature that prompts an insight into the changing conditions which underlie the exercise of personal legal status. These conditions could be described as a large-scale technology-driven social experiment [Ceschin F., 2014]. It should be noted that in the context of this study an experiment is understood more broadly as an activity with unknown and unpredictable outcomes — not as a fixed sequence of actions and not only as a method of scientific investigation — and as a source of experience and empirical data[7].

---

[6] Inrupt, a company owned by the British researcher Timothy Berners-Lee, creator of the World Wide Web, has announced the issue of the proprietary corporate version of Solid, a software platform for Internet data storage and exchange, as reported by the Techcrunch. According to the platform developers, this new version will allow public authorities and businesses to develop web applications for full control of users over their data. Within the Solid ecosystem only end users will decide what data to share, with whom and on what terms. Berners-Lee believes the Internet of the future to be decentralized and free of control by Big Techs such as Facebook, Google or Amazon over the accumulated data. Available at: URL: https://www.cnews.ru/news/top/2020-11-09_otets_interneta_predlozhil?utm_referrer= https%3A%2F%2Fzen.yandex.com (accessed: 12.01.2020)

[7] Ideally, the method of technical experiment should exclude random factors but the social sphere which increasingly spills over into the technological one cannot be fully integrated into the ideal model of experiment. The current processes could more justifiably

The controversial nature of the assertion will require to answer the following questions:

what makes the current experiment, once admitted to be such (a lack of its official announcement does not mean that it does not take place), so different from other technology-driven social processes of the past (including all technological achievements ranging from electric power to nuclear power generation and from space exploration to wide use of food additives);

why is it important to assert the experimental nature of innovations at this stage of development of law and legislation;

what are the legal features of technology-driven social experiment and its impact on the legal status of a person as the most vulnerable subject of social relationships;

what directions can the application of legal experiment and experimental legal regimes take.

1. Features of the Current Technology-Driven Social Experiment and Their Manifestation in Law

The current stage of technological revolution (TR) also described by some authors as technological change [Pashentsev D.A., Zaloilo M.V., Dorskaya A.A., 2021] differs primarily by its coverage (both in terms of the territory and the number of persons) and the pace of its dissemination, only to give rise to the problem of space-time parameters related to the exercise of law. Addressing this problem may give an answer to the question of efficiency of legal provisions to overcome the backwardness (inertia) of law and legislation compared to the pace of social and technological processes [Valverde M., 2015]. In fact, the global outreach of the Internet (as the basis of digitization and technification) owes itself to the uncertainty of its jurisdiction and enormous number of transactions per unit time in the context of its key principle of "unsolicited innovations" (making it possible to anyone, not just specialists, to change the open source code). There is a process of "innovation cycle compacting" when time between the acquisition of new knowledge and the creation and marketing of new technologies, products, services is considerably shorter.

adopt the mode of so-called random experiment based on the concept of random experience and could correspond to real-life test with a high probability that the outcome will be still unpredictable.

This has largely determined a shorter length or a total lack of validation of innovations — a required stage of diagnostics and study of outcomes to be planned and performed in the course of any experiment in its traditional (technical and scientific) sense. This stage almost instantly spills over into legal practices where the most problematic and conflict-prone situations reflecting social responses to the use of technologies are first identified and then summarized.

Importantly, legal practices have limited potential here because of the same uncertainty of jurisdiction and problems to identify the responsible party. However it is currently the only guaranteed mechanism for protection of individuals rights and liberties which supports the emerging trend for segmentation of the web within the national borders, only to refute the hypothesis of destruction of hierarchical links between modern society and state as a result of the expansion of the global information and telecommunication network [Castells M., 2016].

What also makes the current TR so distinct is the involvement of all spheres of life — science, culture, education, health, energy, governance, business, ecology and agriculture — in the processes of digitization, something that directly impacts the personal legal status in all its manifestations. Previously, it was possible to more clearly identify a sector or other field of innovation to distinguish certain related elements (and, therefore, areas of responsibility) such as subjects, dates, outcomes etc.

Serving as an umbrella for other spheres of life, digitization now dictates the rules (including purely technical) to determine their development. While there is indeed a digital gap, inadequate coverage of the population by digital services is definitely considered to be a disadvantage and a problem to be addressed by the government. Moreover, despite the internationally declared principle of equal protection of offline and online rights, the underlying mechanisms have not been clearly defined (except traditional legal action which, as was mentioned earlier, is not always effective in the online context[8]).

[8] For example, according to the terms of service of social media (in 2006–2010 when they actively emerged), personal data are outside the jurisdiction of the user's (party's) state of residence. At the same time, all claims, disputes and lawsuits the user/party might bring against the social media's management are considered at the management's location. Under the terms of reference of VKontakte and Facebook, all disputes involving the management, will be governed, respectively, by the law of Russia and that of the State of California. Obviously, it is impossible for most users to take part in legal proceedings outside their state of residence.

An important distinction of the current technology-driven social processes is informatization, that is, data-based expression and data-based documentation of all of the said processes. The data component has become an integral and to a certain extent natural and even constituting part of digitization underpinned, as one might recall, by the worldwide information and telecommunication network, only to create another risk related to inadequate knowledge of data aspects including legal ones.

Information does not only "permeates" [Tikhomirov Yu.A., Puliaeva E.V., Khludneva N.I., 2012] all spheres of social relationships to follow people through their lives but also becomes a commodity in circulation which, in its turn, is a key trait of information society [Shvetsov A.N., 2011]; [Lazarev V.V., Gadzhiev H.I., 2020: 53–79]. Meanwhile, its properties are considerably different from those of commodity. Information cannot be completely disposed off, even when it changes hands for value; it is practically indestructible; and there is no protection from its dissemination and distortion, especially in the Internet which was designed to store and transfer information without strictly pegging it to its holder.

Thus, the properties of information do not allow to confidently treat it as subject to control and regulation, that is, traditional means of ensuring the rule of law. Moreover, innovative studies in natural sciences suggest to view information as a state of aggregation of matter along with liquid, hard and gaseous states as it is quite measurable (in bits, bytes etc.) thanks to new information technologies. This hypothesis was proposed by Melvin Vopson, a British physicist, who believes that as life becomes increasingly digital, more physical matter — oil, silicon, carbon — is required to satisfy our needs in computing power and data [Vopson M., 2020]. Moreover, he has proposed to consider the bit — a unit of data measurement adopted in the digital environment — as a kind of elementary particle and estimated that in the near future there could be as many of these particles as molecules.

Even without judging the probability of such developments, it is certain that information can move from the sphere of documentation and formalization (first of all, in legal terms) of processes, phenomena, statuses, events etc. into the sphere of data features naturally attributable to a subject/object. This could cause a change in the effect of law on the information component of social relationships. This change is now hard to predict, only to raise the question of unpredictability of legal status of persons in the data environment — for example, in individual decision-making [Casey A., Niblett A., 2018] based on a large amount of personal data

using non-transparent algorithms — which, in its turn, can contradict, as some authors believe, the fundamental principle of the rule of law [Tikhomirov Yu.A., Kashanin A.V., Churakov V.D., 2021: 86].

This can also substantiate the risk-based, experimental nature of activities in the Internet when the development of social processes is hinged on a phenomenon inadequately explored from a legal perspective. In other words, one has yet to fully understand the properties and theory of information as a whole from a perspective of traditional legal concepts and values.

Informatization and overall coverage of social relationships discussed above could be counted among the factors which define the specifics of the experiment as a technology-driven one. The social component of modern technologies has largely ensured the rapid pace of dissemination and deployment of digital innovations, and has set the development vector of economic, political and legal practices. It is the convergence of society and digital technologies that has defined the characteristics of a civilization identified as digital in recent studies [Tikhomirov Yu.A. et al., 2021]; [Kirsanov K.A., Popova S.A., 2020]; [Prohanov A.A. et al., 2020]; [Astafieva O.N., Nikonorova E.V., Shlykova O.V., 2018], only to raise the question of social implications of technological development.

Lastly, what makes the current stage of technological change really different from all previous — let's call them local — stages (in terms of spheres, territories, subjects, products etc.) is a new round of rethinking the ratio between control and freedom emerged in the course of evolution of law and legislation. This ratio might have seemed to be strongly embedded in fundamental documents on rights and liberties nationally and internationally; it assumed both self-imposed limitations of states including for protection of individuals against arbitrary action and a clearly defined measure of freedom allowing to assert a phased transition to a democratic and rights-based constitution.

Meanwhile, the development and dissemination of information technologies and formation of an information (postindustrial, programmable) society as a whole have turned out to involve complex legal processes related to reassessment of the priority of fundamental rights and liberties that might be legitimate at the time of change of a social order. It is primarily the (continued) search for balance between public and private interests which is at stake. Thus, some authors state that "despite the declared constitutional value — ensuring a balance between private and public interests — the Constitutional Court of Russia recently prioritized the protection of public

interests as regards collection, storage and provision of people's personal data to competent officials and public authorities without their consent, as well as the requested deletion of personal data previously provided by individuals to health institutions or connected with prison sentences" [Lazarev V.V., Gadzhiev Kh.I., 2020: 45].

Active legal work is under way to address these problems. For example, the plenary resolution of the Russian Supreme Court of 20 September 2018 (No. 32) "On Amending the Plenary Resolution of the Russian Supreme Court No. 11 of 28 June 2011 "On Legal Practices on Criminal Cases Related to Extremism" features a detailed explanation of the criteria for considering and resolving cases of the said category at courts based on the right guarantee priority and with a view to the so-called pro rata principle in assessing possible restrictions [Lazarev V.V., Gadzhiev Kh. I., 2020: 107–108].

This is also compounded by other problems such as the balance between the priority of protecting freedom of speech and the right to be forgotten, the right to anonymity and the right to reliable information, the freedom of expression and the right to protection of privacy, the freedom of economic activity and the right to data protection. Apart from academic discussion on making up a new catalogue or even whole generation of rights [Talapina E.V., 2019]; [Varlamova N.V., 2019], one of the key issues of which is to substantiate the difference of innovations from the existing and established legal imperative, it is important to address the problem of maintaining the legal values and institutions established over the whole period of evolution which ensure protection of individuals rights and liberties.

In particular, the national security interests are not questioned when certain limitations are imposed on economic agents, with tighter controls perceived by them in most cases as necessary[9]. However, the situation is not so straightforward when, for example, determining the ratio between the right to creative freedom (or economic activity) and the right to protection of privacy.

It is worth noting a problem related to the discussions of the end of the era of privacy [Levin A., 2017]; [Rubinstein I., 2013]; [Legkodimov N.,

[9] In particular, the introduction of the status of critical data structure agent imposing extra duties and restrictions on private entities in communications has become legitimate as web-based services have expanded into critically important areas such as health, energy, transport etc.

2019], with privacy, one of the core rights enshrined in today's fundamental legal documents, being "dissolved" in a new technological environment[10]. Despite the fairly detailed law on personal data protection and the instruction to use only anonymized data[11], it has given rise to a wider problem of the so-called super (hyper) personalization [Swati S., 2019] and even individual regulation based on it [Omri Ben-Shahar, Porat A., 2021]; [Busch C., 2019].

Such novel trends both in law and social development have to be extensively studied, with the data on effects of technology (once put to use) to be accumulated, assessment of outcomes weighed etc. Meanwhile, in order to keep the established legal values, one needs to constantly refer to the legal subject category and, first of all, person as the "primary holder of activity".

The uncertainty faced by law in the digital age largely stems from problems associated with the legal subject as the primary holder of activity and the recipient of regulatory instructions not easily definable in the virtual environment due to the aforementioned reasons. The answer to the question "who has the capacity, ability and obligation to control information flows, and could be liable for implications of the use of technologies" is still to be found and, if correct, will probably determine the success of the rule of law in the digital world.

This makes it important at this stage of technological change to establish the experimental nature of processes involving the population at large and practically all legal subjects. This will allow to develop an approach matching the extent of legal and technological uncertainty around the development of society and state, and also increasing public awareness of the conditions shaped by the expansion of technological civilization.

---

[10] Art. 12 of the Universal Declaration of Human Rights (adopted by the UN General Assembly on 10 December 1948); Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) (adopted in Rome on 4 November 1950); Report of the UN High Commissioner for Human Rights "The Right to Privacy in the Digital Age" (adopted on 10–28 September 2018 at the 39th session of the UN Human Rights Council); COVID-19: Toolkit for Member States — Council of Europe. Respecting democracy, rule of law and human rights in the framework of COVID-19 sanitary crisis (SG/INF(2020)11) (adopted 7 April 2020);

[11] Federal Law No. 152-FZ "On Personal Data" of 27 July 2006; Roskomnadzor Order No. 996 "On Approving the Requirements and Methods for Anonymization of Personal Data" 5 September 2013; Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EU) No. 45/2001 and Decision No. 1247/2002/EC» (GDPR; adopted in Brussels on 23 October 2018.

In other words, it will help overcome the arising information society paradox where despite enormous increase of data, delivery methods and the number of data exchange devices, legal subjects know so little on the essence of events, their legal status and opportunities for its protection that this questions the validity of the right to freedom of information as such (in the sense established in the constitution and internationally acknowledged).

Thus, formalization of legal subjects' "imperfect knowledge", in particular, of their legal status will give an impetus to the development of the legal basis for protection of person in an information society and will help identify the methods for legal guarantees to be ensured by public and private agents who, as parties to the experiment, will be at least willing to review, adjust and improve the products (innovations) to be developed.

Another argument confirming the experimental context of the current stage of evolution could be its transitional nature matching today's technological change closely related to social processes [Pashentsev D.A., Zaloilo M.V., Dorskaya A.A., 2021: 165]. Like any other "time of change", the current stage is characterized by distinctive instability, uncertainty and increasingly tense social relationships whose implementation depends, in particular, on the change of "players" and "rules of the game" imposed from above (or emerging in the course of self-regulation).

It may well be that such "transitional stage" will turn out to be permanent as the ongoing processes accelerate, with each structure's centenary lifecycle and 50 years of economic domination giving way to much shorter and quickly alternating periods. As a result, the only permanent thing will be changes, only to require ongoing adaptation of the legal mechanisms to innovations (probably involving a review of the legal framework).

It is worth noting that regulation of experiments is not a new thing for legal practice and primarily concerns medicine. For example, there are rules for different medical tests enshrined in special codes of good conduct (Nuremberg Code of 1947, Helsinki Declaration of 1964, Russian Code of Good Conduct in Medicine of 1994, Code of Medical Ethics of 1997). In this area, the participation conditions are at least established as regards knowledge of expected outcomes, possibility to quit the experiment at any stage, compensation in the event of negative outcome etc.

The institution of insurance can thus become especially important and gain not only applied but also deeper value-driven development since it will apply to a possibly wider range of legal subjects and life spheres involved in experimental activities.

2. Effect of Legal Attributes of the Experiment on Personal Legal Status

In the current context, a number of legal attributes of such an experiment following from its social component could be distinguished. Among these, it is important to identify:

uncertain jurisdiction (as mentioned previously) which prompts a need to identify new international legal controls and which levels off the legal guarantees established within the national borders in a number of cases;

trend for erosion of responsibility, emergence of the so-called distributed responsibility matching the networking structure of the core technological resource (global network) and the special category of subjects in the experimental sphere;

"mobility" of legal statuses of the subjects who have an option to choose their own legal status depending on how the dispute develops[12];

emergence of a body of new rights and liberties associated with the new technical, economic and social opportunities brought about by innovations;

combination and in some cases competition of the legal and contractual regulatory frameworks related to multipronged development of technologies and their social, primarily legal adaptation/regulation. In this context, the conventional term "contractual framework" means the rules of conduct of digital innovation users established by private subjects (developers etc.) that does not provide for freedom of action or possibility to change the terms of such contract/agreement. This is also a kind of legal attribute of the experiment requiring an insight into the nature of the "contract" to see whether it is compatible with the known private law concepts which guarantee the exercise of rights and liberties.

Identifying a jurisdiction in the Internet as the initial environment for further digitization of social life was among the first problems faced by legal theorists and practitioners. Remarkably, the fundamental international instruments in this sphere did not deal with the issues of jurisdiction despite declaring wide ranging support for expansion of digital services. Thus, the

[12] In this regard, a case handled by Russian courts (No. A40-18827/17-110-180) is of interest. VKontakte, a limited liability company, brought legal action against DABL, a limited liability company, for protection of exclusive related rights to a database which raised the issue of determining the special legal status of the parties which actually affected the outcome of the case.

Okinawa Charter on Global Information Society provides for a need to search for effective political solutions to immediate problems such as preventing attempts of unauthorized access and dissemination of computer viruses. As a key element of its strategy, the Okinawa Charter focuses on ongoing efforts to ensure *universal* access and a *global* approach to dissemination of technologies and knowledge.

Regional segmentation of jurisdiction (within the borders of transnational associations) has likewise failed to become a general model to address jurisdiction problems as in some cases it envisaged a transfer of a part of national sovereignty, something that many countries were reluctant to do.

As a result, the Internet's national segments tend to separate, with important portals concentrating within the national domain space as confirmed by findings of cybergeographic studies [Zook M., Poorthuis A., Donohue R., 2017]. It is largely due to the fact that streamlined national mechanisms of procedural and substantive law applicable at least within the national jurisdiction still prove to be the most effective method of providing guarantees in the cyberspace.

Guarantees decline not only because of jurisdiction issues but also as a result of new approaches to the institution of legal liability which has specific features in the experimental context. While transformation affects all legal institutions across the board, legal liability is the most important of them, with the effectiveness of all other rules depending on it. The concept of so-called distributed responsibility[13] to match the Internet with its distributed network-based social technological structure already assumes a lower amount of guarantees related to its implementation. The difficulty of identifying the liable (responsible) subject to enforce the performance of socially important functions is aggravated by technical backwardness of control authorities and a dilemma to what extent the authorities may interfere with natural social processes taking place on a technological platform.

While no straightforward solution to these problems has been found, there is a global trend for tighter government control which does not mean, however, that self-regulation, a characteristic trait of the innova-

[13] This issue was studied abroad, in particular, at the 2017 Goteborg International Conference on distributed responsibility in times of big data and the Internet of things. Available at: http://is4si-2017.org/program/workshops/distributed-responsibility-times-big-data-internet-things/ (accessed: 25.10.2019). It was noted that there was a rapid increase of data volumes whose predictive analysis determined their impact on a wide range of spheres: military and civil surveillance, social robot technology, online economy, work, health and education, management and control of the Internet of things, intelligent road traffic control systems, intelligent power systems and a variety of financial systems.

tion sector, has failed. Moreover, a number of large and authoritative platforms possessing adequate technological resources — for example, in the Internet — have demonstrated that their owners had quite good legal sense and in absence of rules made serious efforts to protect the rights of social media users, for example, in situations of technical failure causing a possible large-scale leakage of personal data.

Not least important is the problem of correlation between rights and duties as well as liability that is being explored from a perspective of technization of social (including legal one) life. It is this correlation that ensures a necessary degree of freedom underlying law as a whole. Moreover, it can be regarded as an element of the personal legal status which is not only a set of rights and duties but complex structural phenomenon whose effectiveness depends on the right match and mutual influence of its parts both in real life and in the process of enforcement.

The study of the institution of duties and the responsibility they assume has taken a course aimed at exploring the processes taking place in network-based and technologically distributed structures. Such structures assume building and further strengthening of horizontal links between subjects. This has given rise to the term "distributed responsibility" to be analyzed with a view to possible individualization of regulation, developing "networking" approaches to law and specific technology-driven social interactions.

Distributed responsibility (diffusion of responsibility) could be applicable to subject of legal relationships in the Internet as a distributed structure, as well as to other technization processes largely spontaneous and uncontrollable at the stage of deployment. In this case, it may be principally important to answer the question whether the mechanism for distribution of regulatory burden resulting in lower duties imposed on each subject is justified. Obviously, this will require extensive theoretical studies.

This problem has been studied internationally to place responsibility into an increasingly complex and dynamic technology-driven social environment [Simon S., 2014: 145–149][14]. A special focus has been made on the responsibility attached to cognitive processes, a subject discussed in philosophy as epistemic responsibility. In this regard, two viewpoints have emerged: 1) an individualistic perspective focused on individuals within the framework of dynamic technology-driven social epistemic systems,

[14] This issue was at the focus of the 2017 Goteborg International Conference on distributed responsibility in times of big data and the Internet of things. Available at: http://is4si-2017.org/program/workshops/distributed-responsibility-times-big-data-internet-things/ (accessed: 10.06.2020)

and 2) governance perspective focused on how systems and environments should be designed to make people act responsibly (this approach is close to the prospective responsibility theory pursued in jurisprudence [Hart H.L.A., 1949]; [Saveliev Yu. M., 2015]; [Bortnikov S.P., 2012]).

The mechanisms and effectiveness of distributed responsibility of subjects should reflect the legal nature of technization processes where legitimate interests of subjects are closely intertwined and interrelated, opportunities for protection of rights and liberties are reduced due to legal and technological uncertainty while the development occurs largely through and based on self-regulation demonstrating a high degree of performance, once all parties are proactive.

Based on the studies in various fields — for example, philosophy, computer science, robot technologies and arts — there is a discussion of the need to achieve the following objectives:

formulate an adequate concept of distributed responsibility applicable to artificial systems in the future;

establish a ratio between human free will and control replaceable by non-human agents;

what this could mean for responsible application of specific technologies such as social robots, intelligent homes, civil and military drones, driverless cars or financial technologies;

how Big Data and Internet of things challenge the future of responsibility in social structures such as military command chains, social media communication, E-governments, marketing or education.

The problem of legal guarantees is directly related to the issues of efficient performance of duties and responsibilities and becomes especially urgent because of technization of social life. Besides, the issue of legal guarantees as something not explicitly incorporated by the classical theory into the legal status but believed to be inseparable from it proves to be the most complex, once we need to identify a subject capable of ensuring them.

At the same time, there is a problem of "overburdening" the legal status by making a subject already burdened with a number of functions assume more duties. This problem stems, in particular, from multiple sectoral regulation. Thus, the legal status of website owners and data dissemination organizers within the framework of legal relationships in the Internet is established by the federal law related to the information branch while that of data mediators — related to the civil branch.

The trend for "erosion" of responsibility relates not only to the issue whether this institution fits the distributed system where digital transactions take place. It is also a consequence of the need to reduce unfavorable implications for those who generate and introduce innovations. In the context of the study, these persons could be referred to as experimenters, that is, subjects fully responsible for the start and the course of an experiment but to a lesser extent for its implications. As this trend manifests itself in the attempts to shift the burden of responsibility from the subject to the object of activity [Sinitsyn S.A., 2020], jurists are discussing a possibility to introduce legal capacity (and independent responsibility) for robotic and artificial intelligence systems etc. [Yakovlev V.F., Khabrieva T.Ya., Andreev V.K., 2017]; [Blazheev V.V., Yegorova M.A., 2021].

Lower responsibility on the part of "experimenters" can be also observed in certain terms of service of major web resources where it is said, for example, that the management of social media is not responsible for failures and data loss nor for implications of changes to functionality etc. Meanwhile, such problems are not at all exceptional: for instance, in March 2012 a software error resulted in all emails of *Facebook* users becoming accessible for 30 minutes while in May of the same year a security breach allowed to read users' private messages, with a vulnerability enabling hackers to easily access user profiles being later identified [Steinschaden J., 2012].

Another trend to develop an approach to responsibility is to apply the status of a high-risk source owner to developers of the so-called complex software products which affect the operation of major entities [Kryzhanovskaya A.A., 2010]. While only civil liability is meant, the approach itself reflects the context of innovative activities whose negative implications cannot be adequately predicted.

While the implications of software and hardware failures remain to be treated as risks assumed by end users, the only guarantee can now be the "right to know" that the innovative system is not optimized, that it is simultaneously tested as an experimental product and deployed while its implications may have a delayed effect and will require to be specifically studied and responded to.

The next legal feature of the current technology-driven social experiment is a situation of uncertainty faced by legislators in the process of formulating terms and definitions which determine legal statuses and modes involved in digitization. The uncertainty is due to the fact that at the time of drafting a regulation it is impossible to accurately identify the features of a subject or object involved in the innovation sector. These features may

not be obvious to subjects themselves whose functional development follows the law of technology.

Definitions found in law — data mediator, website owner, search engine, virtual currency, blogger — while setting a general trend for associating subjects with certain areas within the innovation sector, leave open the question of who and what they cover. While a variety of opinions was expressed on each of these terms, some of them have adapted to regulation while the other did not stand the test of time and failed to become current in legal practice. In particular, Federal Law No. 97-FZ "On Data, Information Technology and Data Protection" of 5 May 2014 and specific regulations on streamlining data exchange through the use of IT networks (the so called Blogger Law) was revoked. While the term has remained, its legal definition was gone together with the law itself which turned out to be not effective enough as applied to the blogosphere.

Words such as token[15], mining[16], provider[17], cybersquatting[18], messenger[19] can be found in regulations and enforcement documents. In some cases, the authorities have to use the terms not defined or even mentioned in the law. This reflects a new trend in legislation when a systemic approach to terminology is being transformed into a more flexible, ad hoc approach matching the extent of uncertainty, pace of technological change and to some extent the self-regulation mechanisms emerging both among economic agents and within the technological community. In this case, attaching a legal term to a subject can be considered as a starting point in

[15] Bank of Russia standard "Security of financial/banking transactions. Applied software interfaces. Ensuring security of financial services as openid connect client initiates authentication flow via dedicated channel. Requirements" STO BR FAPI.PAOK-1.0-2021». Came into force under Bank of Russia Order No. OD-15 of 23 July 2021.

[16] Chamber for Patent Disputes Opinion of 26 June 2020 (Annex to Rospatent Decision of 10 July 2020 on Application No. 2018726768/33) "On withholding state registration of the given designation as a trademark".

[17] See, for example: Kemerovo Office (FAS of Russia) Resolution of 24 November 2021 on case No. 042/04/14.3-1640/2021; Yaroslavl Office (FAS of Russia) Resolution of 12 May 2021 on case No. 076/01/16-923/2020; Chuvash Republic Office (FAS of Russia) of 30 March 2021 on case No. 021/01/ 10-709/2020. It is noteworthy that while the law contains the definition of a hosting provider (para. 18, Art. 2, Federal Law No. 149-FZ "On Data, Information Technology and Data Protection" of 27 July 2006, it does not cover all features of subjects providing web services.

[18] See, for example: Supreme Court of Russia Determination No. 305-ES20-16127 of 29 October 2020 on case No. A41-85820/2019.

[19] See, for example: Action Plan ("roadmap") "Creating enabling environment for development of information technologies" (approved by the Russian Government on 9 September 2021).

defining its legal status to be developed and specified rather than the final stage where the rights, duties and position in the social relationships system are clearly established.

An illustrative example of dispute resolution is the case involving V Kontakte vs. Dabl LLC[20] where the defendant was able to choose its legal status by referring to loosely worded legal definitions, only to finally win the case. Once recognized as a search engine (at the retrial stage after a detailed technical examination), Dabl LLC managed to evade the liability for using the database of the plaintiff, a major national social media provider. Moreover, the defendant initially claimed to be a data mediator which coincided with the nature of its activities. However, since this line of defense did not yield definite advantages in the dispute, the argument was reversed.

The personal legal status — in this case, that of the V Kontakte users — was also indirectly invoked as the defendant claimed its rights to the data base built up to a large extent with the data users upload to their pages. The question of protecting user rights where the data posted to a social media is used by a third party (in this case, the defendant) was not further explored because the lawsuit alleged violation of exclusive rights to the database. This shows an ambiguous position of users who are not simply recipients of a service but legitimate parties to the data exchange, with the value of the resource (in this case, a social media) as a whole depending on their number and engagement.

This functional "mobility" of the parties to the information process will also determine the mobility of their legal statuses manifested in the multistakeholderism principle applicable primarily to the virtual space. In a wider sense this principle can also be used in the technological innovation sector. It is characterized by a high degree of interdependence of subjects engaged in web-based activities. On 10 June 2019 the Secretary General's High-Level Panel of Digital Cooperation published a report entitled "The Age of Digital Interdependence" in which it was noted that as computer technologies develop, increasingly more users join the worldwide web, with the number of transnational linkages growing annually. Moreover, the report stressed the transformational impact of digital technologies on social, economic, political and cultural spheres of life, that is, those laying the foundation for human development.

Due to a high degree of subjects' interdependence and mutual influence, their legal statuses become transformed as a result of:

[20] Case No. A40-18827/17-110-180.

combination (for example, when technical capability and control functions are combined depending on technical capabilities to affect technological processes or when the use of innovations becomes creative to the point that one becomes able to independently develop a technology, in particular, based on open source codes);

intensification due to a need to perform public functions to maintain law and order and ensure data and national security. This is clearly manifested in the performance of public duties and responsibilities when private law subjects assume certain functions, for example, to participate in the protection of key infrastructure or training exercises involving activities to perform training missions in a specific situation of threat to sustainability, security and integrity of web operations;

coalescence[21] (merger of elements within a mobile environment) where the features and functional association of specific types of subjects cannot be clearly identified due to wide legal definitions applicable to them. Because it was the data sector that gave a decisive impetus to the current technological advance, a relevant example could be the situation where the same subject combines the statuses of a website owner, data mediator, data dissemination organizer and search engine. The said statuses could be established in different branches of law (data law for website owners, civil law for data mediators) but involve legislative regulation of subject's activities in the global information and telecommunication network.

The trend for "mobility" of legal statuses involving their transformation will require further research, first of all theoretical, to propose justified criteria of such transformation, preserve the historically established legal values and develop new legal mechanisms abreast of time.

Regarding the transformation criteria of the legal status of subjects (that is, the indicators capable of justifying this transformation from social, legal, technological perspectives) the following could be proposed:

conformity with statutory principles and provisions;

[21] The term "coalescence" is used to underline the difference between the processes of merger and combination of legal statuses. Coalescence is a merger within a structure represented in this study by the legal status of a subject who simultaneously performs the functions, for example, of the website owner, data mediator and data dissemination organizer. In contrast, combination takes place when one group of subjects is able to perform the functions of the other, that is, when the legal status emerges as a result of simultaneous performance of support and control functions as well as a result of network use. This transformation of legal status becomes transversal, as it were, and is regarded in view of prior categorization of subjects as persons who use, support and control the Internet.

changing role in the system of legal relationships (in particular, an increase in technical capability support or control functions);

opportunity to control technological processes related to the exercise of the rights and duties of subjects;

clear identification of the purpose of transforming a subject's legal status in view of legitimate interests of other subjects;

degree of influence (economic, political, information, technological) on the legal status of other subjects;

degree of the subject's vulnerability to technological (information, political etc.) impact.

While the process of transformation of legal status can affect rights and duties (in the form of both contractual and legislative regulation), the legitimate interests (as a conceptually identified element of the legal status) should be preserved and cannot be subject to outside change because they essentially reflect the subject's internal motivation.

A study of the emergence of a body of new rights and liberties as a feature of the experimental state of society merits a special focus. New technical, economic and social opportunities created by innovations invariably bring about new rights. Many policy definitions of rights contain a key word "opportunities" as something potentially able of being translated into rights.

However, not all opportunities are backed by guarantees and clearly correlate with duties — far from it — since they require to identify the respective responsible subject. While factors of such transformation need to be carefully established in the theory, it is already possible to identify among them the social justification and the implementation of legitimate interests and opportunities of specific subjects (both public authorities and private individuals) to guarantee these rights.

The widespread term digital rights used domestically in the Civil Code of Russia obviously has a wider connotation and applies to a broad range of rights and liberties exercised in the Internet.

The rights related exclusively to the emergence of Internet and development of social relationships in a digital environment include:

Internet access right as a whole (as a result of the general and presumably global trend for digitization, the Internet was recognized a social good and it was proposed to establish the statutory right of online access which

explicitly assumes the government's involvement in order to be guaranteed. This issue is still debated, especially in the context of pandemic when the importance of the global web has grown exponentially as more user transactions went online. Moreover, the Internet demonstrated the willingness to increase the data traffic (data on major operating failures even during the total lockdown when a large part of the population had to work remotely) and proved to be technically fit to make up for the lack of physical interaction. But while the technical and organizational conditions to formalize the right of access are there, a high degree of uncertainty around the web development prospects does not yet allow to propose a straightforward approach to establishing such a right;

data protection right (discussed due to the exponential increase of volume and detail of data whose psychological and social impact is yet to be adequately studied but negative implications are already there. These implications call for a "search" for certain new opportunities for users to establish the rule of law in the virtual environment. In this case, the right can be characterized as a justified claim from a perspective of the non-classical theory which complements and expands the understanding of the object of rights [Tumanova A.S., Kiselev R.V., 2011: 41]; [Heffe O., 1994: 248]);

network neutrality enabling right (that is, technically ensuring the same data delivery quality irrespective of the content, meaning, addressee etc. As the network neutrality principle is being recognized as important for overall system operation, it is gradually moving from self-regulation (as this opportunity was initially there) to the legislative sphere capable of better securing this opportunity[22]);

right to a domain name (covering a large number of private law issues while being related exclusively to the worldwide web's architecture);

subject's right to manage personal data in the Internet (actually meant to make up for the aforementioned "technical debt" reflecting a lack of opportunities to exercise the established rights such as the data or privacy protection right)[23].

[22] For example, Law of Brazil No. 12.9652014 of 23 April 2014 has established a system of civil rights in the Internet (Marco Civil da Internet).

[23] This conclusion could be confirmed by the emerging trend to change data management policy in the Internet as the most urgent problem for protection of digital rights and liberties. Inrupt, a company owned by the British scientist Timothy Berners-Lee, creator of the World Wide Web, has announced the launch of a corporate version of its software platform which, as developers claim, will allow users to gain full control of their own data. Within this ecosystem only end users will decide, what data to share, with whom and on what terms. The scientist believes the Internet of the future to be decentralized, that is,

We believe digital rights and liberties can be defined as broader opportunities for individual and collective subjects to exercise the whole range of acknowledged rights and liberties, as well as new opportunities (justified claims) for acquiring tangible and non-tangible goods through legitimate use of the global information and telecommunication network.

The nature of such rights is predetermined both legally and contractually, that is, combines public and private law principles of emergence and regulation, as well as technological peculiarities of Internet operations, only to result in certain risks involved in their protection.

A combination of public and private law principles applicable to regulation of social relationships related to the innovation sector as a juridical feature of the current technology-driven social experiment leads to a model conventionally called "supervised self-regulation". The current explosion of new ICTs largely owes itself to freedom of private enterprise. At the early "testing" stage this form of expansion involving minimum restrictions was justified and convenient.

However, as innovations spread out the initially achieved success has brought about the awareness of the underlying complications and a need for regulation by public authorities. This issue is also raised by representatives of the technological community apparently willing to adopt regulatory mechanisms capable of adapting the algorithms to society and thus contribute to further development of science. A skeptical attitude to the applicability of legal controls to the technological sector should (and gradually does) give way to the awareness of the need for cooperation between technologies and jurisprudence. Both are the evolutionary achievements of humanity and cannot prevail in modern society possessing adequate historical experience of overcoming any pressure which stands in the way of natural social development.

A certain competition between regulatory principles of public and private law can still be observed as mainly manifested in restrictions which, once introduced, do not always prove to be as effective as expected[24].

While the search for effective legal mechanisms continues, self-regulation is proposing new solutions to the problems which the law has failed to address. For example, the problem of ensuring exclusive rights to works

free of control by Big Techs such as Facebook, Google or Amazon over the accumulated data. Available at: URL: https://www.cnews.ru/news/top/2020-11-09_otets_interneta_predlozhil?utm_referrer=https%3A%2F%2Fzen.yandex.com (accessed: 10.06.2020)

[24] The high-profile cases include the attempts to impose restrictions on Telegram and Twitter as well as penalties on Facebook and Google.

posted online has been partially solved by developing and deploying convenient and accessible platforms proposing content of high quality. Legal provisions and even special institutional mechanisms (such as web police) aimed at prohibiting the circulation of pirated products are also applicable but obviously unable to fully reverse the situation and put it under control.

The attempts to address the issue of web content inheritance is also of interest. While it is still debated among jurists whether to include it into the mass of the succession, treat as tangible or intangible asset (no straightforward answer is there yet), Apple has developed the Digital Legacy function which provides for transfer of data from iCloud to one of the user's trustees in the event of his death.

Thus, the regulation of technologies is still be based on self-regulation taking into account legal formulas which "identify" the problems of adapting technologies to social relationships and set the general trend for addressing the urgent problems of using the expanded capabilities of technological innovations.

The competition of public and private law regulatory mechanisms is gradually giving way to their combination in specific areas of social relationships which is expected to help balance all vested interests involved in adoption of innovations. Moreover, there is a need to preserve the personal legal status as a key indicator reflecting the justification and usefulness of introducing controls in the context of technological change. The acknowledgement of experimental nature of activities will allow not only maintain the existing rights and liberties but also possibly expand their range by introducing more legal guarantees.

Conclusions

Identifying legal features of the experiment under way in all spheres of life is primarily aimed at developing legal mechanisms to regulate social relationships in this context. In this case, the introduction of experimental legal regimes increasingly present in the innovation sector is legitimate and logical. This method of regulation is now necessary and justified while any criticism that legislative imperatives will weaken since public institutions will be unable to take decisions with confidence during the active use of legal experiment is irrelevant as it does not reflect the specifics of general conditions of existence of the state and society.

The problems previously identified in jurisprudence are still there including difficulties of implementing the idea of a legal experiment related to the need to simulate the real legal environment to test proposed solu-

tions (the environmental aspect being definitely vital for the technology sector) and to choose hypotheses to review decisions, assessment criteria etc. [Tikhomirov Yu.A., 2015: 83]. Still unresolved is the problem of distinguishing the impact of experimental factor as such [Yeltsov V.N., 2009], with the issue of legal experiment, its functions, possible limits, special legal guarantees for those affected, clear criteria of when such experiments are useful or necessary yet to be properly studied [Motin S.V., 1999].

At the same time, progress in this sphere is obvious. The adoption of Federal Law No. 258-FZ "On Experimental Legal Regimes in the Digital Innovation Area in Russia" of 31 July 2020 has been a major step towards legal accommodation of experimental activities and understanding them from a perspective of law.

The law is largely directed at corporate agents of innovation, subjects of the experimental legal regime (as defined by the law). Meanwhile, it also covers the personal legal status in a wider sense by establishing the category of "participants to the experimental legal regime" to distinguish the legal status of those initiating an experiment and those directly involved in it, that is, validating new goods and services.

As the first principle of an experimental legal regime specified in the law, it is forbidden to restrict the statutory rights and liberties of individuals, compromise the common economic space in the territory of the Russian Federation or otherwise reduce the right protection guarantees of individuals and legal entities envisaged by the Art. 4 of the Constitution and other national regulations.

This provision confirms the importance of the effective legal provisions in an experimental environment, as well as defines the peculiarities of experimental conditions themselves which require regulation with regard to dates and territory of the experiment (part 3, Art. 6, Art. 7), due regard for the risks related to the use of innovations (p. 4, part 5, Art. 10), compensation of damage to health of individuals or property of legal entities as a result of experimental legal regime including those caused by legitimate actions of subjects to the experimental legal regime (part 4, Art. 5).

Importantly, the law allows to avoid entering into relationships with subjects of an experimental legal regime and to introduce extra guarantees for protecting the rights of those entering into such legal relationships including advice of special regulation (part 7, Art. 5).

Such provisions already reflect the fact the law recognizes experimental nature of activities and of legal status of subjects able later to transform into a full legal status to ensure adequate protection of persons, society and state.

Further development prospects of such approach can involve more variable use of legal experiments. For example, it has been proposed to make virtual worlds a place for testing certain legal formulas for the real world while legal simulators can prove to be useful for "laboratory testing" and more effective, safe and secure real world introduction of certain provisions. Such simulation has been conducted so far experimentally in the area of social science and humanities [Baturin Yu.M., 2017: 27–35].

We believe a broader application field of the legal experiment will respond to the pace of changing social relationships in the context of technological change, help maintain the guarantees of the established rights and liberties, and contribute to the development of well-balanced legal controls.

Moreover, such a system, with analogue communications being preserved, will help overcome an overall negative perception of technology as a dangerous, unexplored and risk-prone phenomenon offering no chance of influence because of its mysterious essence [Heidegger M., 1993]. These concerns were expressed by Martin Heidegger who considered technology to be a resource and a functional element of supply production, only to show that man and nature become resources themselves and thus refute a widespread belief that man is a master of technology and nature and that technology has no impact on nature.

Still more important is to understand the process of transformation of personal legal status from a perspective of future philosophy of law whose emergence will influence the status of persons as legitimate parties to all social and technological processes protected from arbitrary technocratic action and endowed with the right of choice and opportunities to exercise it.

In this case, the personal legal status will be indicative of evolutionary path of modern society capable of further existence, cured from mistakes of the past and protected from future crises.

A stronger focus on the institution of personal legal status, especially in the current uncertain context, is meant to prevent persons from being permanently and fully (or even partially) transformed into test subjects deprived of protection and adequate information of what is going on, and to avoid the worst case scenarios including the aggravation of social and political conflicts and loss of human capital accumulated over centuries and driving the development of legal institutions and provisions.

At the same time, it would be unreasonable to restrict the right of developers to commercialize the outcomes of innovations since it contradicts the principles of progress and could undermine competition and civil

action. It has been underlined in research papers that further efforts are required to search for legal controls that would encourage the high tech development. They should also more adequately unlock the principles and mechanisms of public-private partnership — involvement of the government and businesses in joint projects which neither the government or businesses could implement on their own. These include, in particular, the projects in the area of information and communication and new technologies [Khabrieva T.Ya., 2012: 20].

One could possibly suggest the juridification of technologies involving close cooperation between representatives of the technological and legal communities which ideally should be promoted on the basis of recognition of the priority of the personal rights and liberties.

References

1. Abliazov N. (2017) The technological singularity. A study of conditions of emergence and implications for humanity. Available at: URL: https://mipt.ru/education/chair/philosophy/publications/aspers/a_1xes5v.php (In Russ.).

2. Astafieva O.N., Nikonorova E.V., Shlykova O.V. (2018) The digital civilization culture: new stage of the understanding of future sustainable development strategies. The cultural observatory. no. 15(5), pp. 516–531. Available at: URL: https://doi.org/10.25281/2072-3156-2018-15-5-516-531 (In Russ.).

3. Baturin Yu.M. (2017) Legal violations in online worlds and experimental jurisprudence. In: Papers of international research workshop "Security, conflicts and fight against extremism in Internet: legal aspects". Moscow. P. 27–35. (In Russ.).

4. Bechmann G. (2012) Modern Society: risk-prone, information and knowledge society. Moscow: Norma. 247 p. (In Russ.).

5. Big data interpretation and application in jurisprudence and legal practice (2021) Yu.A. Tikhomirov, A.V. Kashanin, V.D. Churakov et al. Moscow: Yustitsinform. 188 p. (In Russ.).

6. Bortnikov S.P. (2012) The prospective and retrospective responsibility. *Ekonomika i pravo* = Economy and Law, no. 12, p. 47–50 (In Russ.).

7. Boroon L. et al. (2021) The Dark Side of Using Online Social Networks: A Review of Individuals Negative Experiences. DOI: 10.4018/JGIM.20211101.oa34. Available at: https://www.igi-global.com/article/the-dark-side-of-using-online-social-networks/276942

8. Busch C. (2020) Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law. Available at: https://

lawreview.uchicago.edu/publication/implementing-personalized-law-personalized-disclosures-consumer-law-and-data-privacy-law

9. Casey A.A. (2018) Framework for the New Personalization of Law. Computer Science. *Law & Society: Legal Profession.* Available at: https://www.semanticscholar.org/paper/A-Framework-for-the-New-Personalization-of-Law-Casey-Niblett/d0f4605c180ce64d0ff5d-ba7705a5101a0f0c741

10. Castels M. (2016) *The power of communication.* Moscow: Higher School of Economics. 564 p. (In Russ.).

11. Ceschin F. (2014) How the Design of Socio-technical Experiments Can Enable Radical Changes for Sustainability. International Journal of Design, vol. 8, no. 3. Available at: http://www.ijdesign.org/index.php/IJDesign/article/view/1308/650

12. Churgeev V.L. (2015) The technical debt in innovative software projects. *Problemy territorialnogo razvitia* = Territorial development issues, no. 2 (22). Available at: URL: https://cyberleninka.ru/article/n/tehnicheskiy-dolg-v-programmnyh-proektah-innovatsionnogo-tipa/viewer

13. Data protection: comments to legal practices (2020) V.V. Lazarev et al. Moscow: Kontrakt. 174 p. (In Russ.).

14. Digital civilization (2020) Media communications. Web marketing. Lobodenko L., Shesterkina L. et al. Chelyabinsk: University. 770 p.(In Russ.).

15. Digital civilization (2018) Russian and the 21th century electronic world. Prokhanov A.A. et al. Moscow: Knizhny Mir. 288 p. (In Russ.).

16. Digital law (2021) V.V. Blazheev, M.A. Yegorova et al. Moscow: Prospekt. 640 p. (In Russ.).

17. Hart H.L.A. (1949) The Ascription of Responsibility and Rights. *Proceedings of the Aristotelian Society,* vol. 49, pp. 171–194.

18. Heffe O. (1994) *Politics. Law. Justice. The foundations of critical philosophy of law and state.* Moscow: Gnosis Publishers. 319 p. (In Russ.).

19. Heidegger M. (1993) The question of technology. In: The Coming Technological Singularity: how to Survive in the Post-Human Era. Available at: http://www-rohan.sdsu.edu/faculty/vinge/misc/singularity.html

20. Kirsanov K.A., Popova S.A. (2020) Digital civilization. *Mirovye civilizaccii* = Civilizations of the world, no. 1–2. (In Russ.).

21. Khabrieva T.Ya., Chernogor N.N. *Future of Law* (2020) Moscow: Norma 174 p. (In Russ.).

22. Kryzhanovskaya A.A. (2010) *Civil liability for the damage caused by complex software products.* Moscow: Norma, 160 p. (In Russ.).

23. Law and biomedicine (2021) F.V. Tsomartova (ed.). Moscow: Norma. 136 p. (In Russ.).

24. Legal capacity: legal analysis (2017) Papers of XII annual scholar readings. V.F. Yakovlev, T.Ya. Khabrieva, V.K. Andreev et al. Moscow: Statut. 434 p. (In Russ.).

25. Legal environment and man (2012) N.V. Vlasova, S.A. Gracheva, M.A. Mescheryakova et al. Moscow: Yurispridentsia. 249 p. (In Russ.).

26. Legkodimov N. (2019) End of the privacy age. *Vedomosti*. = News, 9 July. Available at: URL: https://www.vedomosti.ru/opinion/articles/2019/07/09/806225-konets-privatnoi-epohi. (In Russ.).

27. Lessing L. (2017) Vast online games need a political structure. Available at: https://mmozg.net/mmo/2017/06/06/professor-lourens-lessing-onlaynovym-mir am-neobhodimapoliticheskaya-sistema.html

28. Levin A. (2017) Has the Era of Privacy Come to an End? *Canadian journal of law and technology,* vol. 15, no. 1. Available at: https://digitalcommons.schulichlaw.dal.ca/cjlt/vol15/iss1/2/

29. Medvedovsky I. (2016) The age of hackers: why privacy is gone for good. Available at: URL: https://www.rbc.ru/opinions/technology_and_media/01/04/2016/56fe59b79a7947bb7cf4b4e4. (In Russ.)

30. Misostishhov T.Z. (2020) The personalized rights and fundamental rights. *Cifrovoe pravo* = Digital right, no. 1, pp. 56–73. Available at: https://doi.org/10.38044/2686-9136-2020-1-4-56-73

31. Motin S.V. (1999) Experimental method in the social and legal environment. Candidate of Juridical Sciences Summary. Moscow, 24 p. (In Russ.).

32. Omri B., Porat A. (2021) *Personalized Law Different Rules for Different People.* N.Y.: Oxford University Press. 256 p.

33. Pashentsev D.A., Zaloilo M.V., Dorskaya A.A. (2021) *Technological change and legal development of Russia.* Moscow: Norma. (In Russ.).

34. Reynolds G. (2003) Nanotechnology and Regulatory Policy: Three Futures *Harvard Journal of Law and Technology,* vol. 17, no. 1, pp. 180–209.

35. Rubinstein I. (2013) Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, vol. 3, no. 2.

36. Saveliev Yu.M. (2015) Concept of legal responsibility. *Pravovye issledovania* = Legal Studies, no. 10. pp. 61–80. DOI: 10.7256/2409-7136.2015.10.1612. Available at: URL: https://nbpublish.com/library_read_article.php?id = 16122. (In Russ.).

37. Shaw J. (2009) The erosion of privacy in the Internet era. Available at: https://www.harvardmagazine.com/2009/09/privacy-erosion-in-internet-era

38. Shvetsov A.N. (2011) *Information society: theory and practice of the emergence in Russia and worldwide.* Moscow: URSS. 277 p. (In Russ.).

39. Sinitsin C.A. (2020) *The Russian and international civil law in the context of robotization and digitization.* Moscow: Infotropic. 256 p. (In Russ.).

40. Simon S. (2014) Distributed Epistemic Responsibility in a Hyperconnected Era. *The Onlife Manifesto*, pp. 145–159.

41. Spitsin I.N. (2021) Juridification of artificial intelligence concept and limits of using AI technology at court. *Lex Russica* = Russian Law, no. 10. (In Russ.).

42. Steinschaden J.(2011) *Social media. Facebook phenomenon.* Moscow

43. Swati S. (2019) Privacy versus personalization. Available at: https://www.the-future-of-commerce.com/2019/01/28/privacy-versus-personalization/

44. Talapina E.B. (2019) The evolution of human rights in a digital age. *Papers of the Institute of State and Law*, no. 3 ,122–146 p. (In Russ.).

45. Tikhomirov Yu.A. (2015) *Law: prospects and risks.* Moscow: Norma. (In Russ.)

46. Tikhomirov Yu., Kichigin N. et al. (2021) Law and Digital Transformation. *Legal Issues in the Digital Age,* vol. 2, no. 2. (In Russ.).

47. Tikhonova S.V. (2017) Juridization of ICT as a driving factor of e-government. Guarantees of Human Rights and Liberties in Today's World: workshop papers. Moscow: Prospect. p. 275–278 (In Russ.).

48. Tumanova A.S., Kiselev R.V. (2011) *Human rights in legal theory and legislation of Russia, second half of 19-early 20 century.* Moscow: HSE. (In Russ.).

49. Valverde M. (2015) *Chronotopes of Law: Jurisdiction, Scale and Governance.* L.: Routledge. P. 668–673.

50. Varlamova N.V. (2019) Digital rights: new generation of human rights? *Collected works of Institute of State and Law,* vol. 14, no. 4. (In Russ.).

51. Vopson M. (1994) The information catastrophe. Available at: URL: https://zen.yandex.ru/media/htech_plus/fizik-melvin-vopson-temnaia-materiia-mojet-byt-informaciei-5f3637ae40616c4c6b9682f1

52. Yeltsov V.N. (2009) Legal experiment in modern Russia. Candidate of Juridical Sciences Summary. Tambov, 25 p. (In Russ.).

53. Zook M., Poorthuis A., Donohue R. (2017) Mapping Spaces: Cartographic Representations of Online Data. In: Handbook of Online Research Methods.

Information about the author:

M.E. Cheremisinova — Candidate of Sciences (Law), Senior Researcher.

The article was submitted 12.07.2021; approved after reviewing 11.10.2021; accepted for publication 01.11.2021

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4

Research article
UDC: 342
DOI: 10.17323/2713-2749.2021.4.34.69

Sharing Radio Spectrum for Research and Innovation

Jos Dumortier[1],
Irina Yurievna Bogdanovskaya [2],
Niels Vandezande[3],
Mikail Yakushev [4]

[1] Timelex Lawyers, Brussels, Belgium.

[2,4] National Research University Higher School of Economics, Moscow, Russia.

[3] Timelex Lawyers, Brussels, Belgium.

[1] Jos.dumortier@timelex.eu.

[2] ibogdanovskaia@hse.ru, ORCID: 0000-0002-6243-4301

[3] Niels.vandezande@timelex.eu.

[4] myakushev@hse.ru

Abstract

In most countries academic researchers have access to advanced academic telecommunications networks and infrastructures to test and demonstrate the results of their research work. These networks are usually funded by national or regional public authorities. To provide access to the academic networks on a wider scale, European and international collaboration initiatives have been taken. For the fixed network environment this may suffice but the situation is different in the wireless context, partly because here, researchers must, in one way or another, obtain spectrum usage rights. Today spectrum usage rights can be quite easily obtained in the restricted territorial space of a testbed. Yet, small-scale testbeds are not sufficient anymore for realistic validation, and the scientific community today needs large-scale field deployments working with the same radio spectrum as the commercial networks and capable of supporting new technologies and services. The evolution from lab testbeds to field deployments is required to increase the validation capabilities for complex systems like connected cars, massive Internet of Things (IoT) or eHealth solutions. Appropriate frequency bands, needed by researchers to carry out, for example, large-scale 5G experiments, are generally allocated via auctions and on an exclusive basis to large mobile network operators.

While it is perfectly feasible for these MNOs to keep dedicated slices for tests and demonstrations in their networks separate from their day-to-day operations without negative effects for the latter, there are few regulatory mechanisms for stimulating MNOs to make parts of their spectrum usage rights available for the academic research community. All EU Member States allow short-term licenses for the use of radio spectrum for research, testing, and experimental purposes, but procedures, requirements, and costs for obtaining such license vary significantly. These national differences do not allow for the creation of a persistent and pan-European network of wireless capacity for research, testing, and experimental purposes. On the secondary market, leasing or transferring radio spectrum usage rights is possible, and procedures seem more harmonized.

Keywords

radio spectrum management, mobile communications research, 5G trials, 5G testbeds, temporary spectrum license, spectrum sharing, spectrum trading, spectrum leasing

For citation: Dumortier J., Bogdanovskaya I.Yu., Vandesande N., Yakushev M.V. Sharing Radio Spectrum for Research and Innovation. *Legal Issues in the Digital Age.* 2021, no. 4, pp. 34–69. DOI: 10.17323/2713-2749.2021.4.34.69.

Introduction

Almost every country today ensures easy access for the academic research community to high-performance electronic communications networks and infrastructures. National research networks (so-called NRENs) already interconnected academic institutions long before the Internet existed [Martin O., 2012]. Today one of their main functions is to connect university researchers and students to the Internet. In Europe, the GÉANT network interconnects Europe's NRENs organisations with a pan-European backbone — connecting researchers, academics and students to each other, and linking them to researchers outside Europe, including to the Russian national research networks. The GÉANT network is essential to Europe's e-infrastructure strategy, supporting open science with a future-proof e-infrastructure and advanced networking services for trusted access. In addition, GÉANT allocates dynamically network testbed resources from real e-infrastructure distributed throughout the GÉ ANT core service area, allowing researchers to define, build, test and re build highly scalable, high capacity virtual networks quickly, easily and cost-effectively. GÉANT Testbed Services (GTS) allow users to easily build high performance heterogeneous virtual environments required for their

experiments. This allows them to focus on the actual experiments and not on the underlying infrastructures necessary to carry out the work. Such flexibility enables rapid prototyping and facilitates early stage innovation in Internet-scale applications and services. Today, NRENs do not provide similar services to the academic research community in the wireless environment. Field trials using mobile networks are mainly hosted by commercial mobile network operators (MNOs), which often do not provide access to the results nor to the infrastructure they have deployed. Yet, due to the growing complexity of mobile networks, the scientific community needs more realistic experimental facilities with the purpose of validating new ideas on networks or services against the expected behaviour. This need is especially critical to study aspects like Quality of Service (QoS) or Quality of Experience (QoE). Research in the context of mobile networks is currently restricted to indoor research platforms built with private or public funding. However, such small-scale testbeds are not appropriate for realistic validation. For instance, they cannot realistically represent a massive number of users in the same radio access point, or thousands of devices for IoT applications, nor take into consideration the complex reality of a real-life deployment. Therefore, the scientific community needs large-scale field deployments working with the same radio spectrum as the commercial networks and capable of supporting the new technologies and services. The evolution from lab testbeds to field deployments is required to increase the validation capabilities for complex systems like connected cars, massive Internet of Things (IoT), or eHealth solutions. In this perspective, the European Commission already supports the aggregation of the experimental facilities, for example interconnecting the current testbeds and field trials.1 The Future Internet Research and Experimentation (FIRE) objective, put forward in the context of the European Union's multi-annual research programmes, has extended, federated, or even created new research infrastructures for ICT in Europe.[2] Some of them support wireless cellular communication, but they are basically for indoor deployments, without connection to commercial operators.[3] Only recently, the European Commission finances feasibility studies for the creation of dedicated wireless service provision for the academic research commun-

[1] Some of these facilities are federated in Fed4FIRE+. Available at: www.fed4fire.eu. (accessed: 22.04. 2020)

[2] Available at: https://ec.europa.eu/digital-single-market/en/future-internet-research-and-experimentation(accessed: 22.04. 2020)

[3] The same problem has been partially addressed in the USA by the SciWinet initiative. SciWinet works as an umbrella to make agreements easier between universities and MNOs to install new equipment for limited use under a master agreement to share the spectrum.

ity in large-scale operating mobile networks. These studies show that it is technically possible to share radio spectrum and network infrastructures between commercial mobile network operators and academic researchers without mutual interference or other negative effects.[4] The problem lies elsewhere, in the readiness of mobile network operators to share their spectrum usage rights and their network infrastructure. This article focuses on spectrum usage rights and the possibilities of sharing such rights from a regulatory point of view. To explain the issue, it is first necessary to understand the basics of radio spectrum regulation.

2. The Basics of Radio Spectrum Regulation

2.1. Characteristics of Radio Waves

Radio is the transmission of signals by the modulation of electromagnetic waves. These signals go out through the air as radio waves. Radio waves are not directional and travel through space in all directions, like ripples on a pond [Donovan J., 2019]. The frequencies of radio waves vary between 30 Hz and 3000 GHz, corresponding to wavelengths between 10000 km and 0.1 mm. Radio is particularly suited for wireless communications as it is "easy to use, has good propagation characteristics, and is relatively safe" [Ellingson S.W., 2016]. The history of this technology goes back to the late 19th century, when Heinrich Hertz proved that electricity can be transmitted in electro-magnetic waves.

The radio spectrum is commonly divided into bands. Within a band, channels are typically intended for the same purpose. A band plan will normally determine how the radio frequencies within a particular band can be used, for instance by establishing the bandwidth of each channel within that band, what type of content can be transferred on these channels, who can operate a channel and under which conditions, etc. The aim of the band plan is to avoid interference and to ensure an efficient use of the radio spectrum.

The lowest frequency bands (between 3 Hz and 3 kHz) are generally used for (sub)marine communications, as they can penetrate seawater. The highest band is mainly employed in astronomy, although other uses — such as for medical imaging — are currently being researched. Typical fre-

[4] One of these studies takes place in the context of the Horizon 2020 research and innovation action "EUWireless" in which two of the authors of this article have been involved. Available at: https://www.euwireless.eu. (accessed: 22.04.2020)

quencies used by GSM networks are 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz.[5]

2.2. Radio Spectrum is a Rival, Non-Excludable Good

Before delving in the regulation of the radio spectrum, it is useful to determine how the radio spectrum can be considered under the classic economic theory of goods [Samuelson P., 1954]. This theory distinguishes four types of goods, characterized by two criteria: excludability and rivalry. Excludability of a good means that one can block the access of certain people to that good, for instance if those people have not paid for such access. An example here could be any type of consumer electronics, such as laptops. Such device can generally not be obtained unless paid for. Conversely, a vendor could also refuse to make a sale. A non-excludable good is then a good from which access cannot be blocked. An example here is a public landmark, which anyone can see, and which cannot be prohibited from being seen. A rival good is a good that can only be consumed by one person at a time. Bread is a typical example of such rival good, as once a loaf of bread has been consumed, nobody else will be able to consume it. Conversely, a non-rival good can be purchased by several persons at a time. The Internet provides a good example of a non-rival good, as websites can be viewed by many people at the same time. The radio spectrum could be considered as a rival good. While the spectrum cannot be depleted — in the way that an ocean can be depleted from fish due to overfishing — it can become congested by the increasing number of mobile devices using the same frequencies [Herter C., 1985]. This results in interference, which may thus prevent the proper functioning of electronic communications services. While newer technologies exist that may limit this kind of interference, the increasing number of devices using the radio spectrum still results in potential rivalry issues — e.g. the presence of several Wi-Fi routers using the same bands in a small local area.

The radio spectrum could in principle also be considered as a non-excludable good. As radio waves are all around us, it is difficult — if not impossible — to exclude someone from using them. Legislation can be adopted to restrict the use of the radio spectrum, but this does not prevent people from doing so. Even when wireless devices are regulated, it is not

[5] Long-Term Evolution (LTE) or 4G technology is generally deployed on the 700 MHz, 800 MHz, 850 MHz, 1700 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 2600 MHz, and 3500 MHz frequencies. 5G technology is expected to use frequencies in the existing LTE range (600 MHz — 6 GHz) and in millimetre wave bands (24 GHz — 86 GHz). Other popular wireless technologies include Bluetooth (operating around 2400 MHz), Near-Field Communication (NFC, operating at 13.56 MHz), and Wi-Fi (2.4 GHz and 5.8 GHz).

unfeasible to obtain or build a receiver for certain wireless communications. Alternative methods — such as the encryption of signals — will have to be used to prevent people from receiving the wireless communication in understandable form.

This rivalrous, yet non-excludable nature of the radio spectrum makes it a common pool resource [Berge E., Kranakis E., 2011]. Such resource, if left unmanaged, could fall victim to what Hardin famously called 'the tragedy of the commons', whereby an unregulated resource could become subject to overuse and overconsumption, thus potentially destroying the resource in the process [Hardin G., 1968].[6] For the radio spectrum, such to some extent occurred in the 1920s, when hundreds of new radio stations took the air and used "any frequencies they desired, regardless of the interference thereby caused to others". As a result, "with everybody on the air, nobody could be heard".[7]

2.3. Objectives of Spectrum Regulation

To avoid this kind of tragedy of the commons, some form of regulation of common pool resources may be proposed. One example is Ostrom's model for self-governing commons [Ostrom E., 1990]. In the context of spectrum management, there is a recent movement arguing in favour of true spectrum commons self-regulation [Brito J., 2006]. Nevertheless, most states have adopted the models Ostrom criticized most: state intervention and private property [Rishabh, 2016]. When using state intervention — also called 'command and control' — the state will adopt a legal framework to determine the frequency bands, their specific uses, the technologies to use these bands, and the administrative authorization of users. This approach centralizes the control and legitimizes certain uses of the spectrum. In more recent years, states have been allocating full control over specific bands to private actors using public auctions. This shift from state intervention to private property came following Coase's assertion that private ownership could lead to a more efficient utilization of the radio spectrum [Coase R.M., 1959].

From a regulatory point of view, the radio spectrum could be compared to a beach. While in principle a beach is freely accessible for everyone, it is possible to establish certain ground rules under which the beach can be

[6] The tragedy of the commons refers to a dilemma described in Garrett Hardin's article. He describes a situation in which multiple individuals, acting independently, and solely and rationally consulting their own self-interest, will ultimately destroy a shared limited resource even when it is clear that it is not in anyone's long-term interest for this to happen.

[7] National Broadcasting Co. v. United States, 319 U.S. 190 (1943).

used — e.g. only allowing swimming in designated areas under supervision of lifeguards. However, it is also possible to give (part of) a beach in private concession to a hotel. In such case, that (part of a) beach can only be used by the hotel's guests. Going back to the radio spectrum: while radio waves can in principle be used by anyone, governments have determined the basic rules for utilizing radio communications. Moreover, states have reserved certain sections of the radio spectrum for the exclusive use of the private sector users that are being awarded an operating license hereto.

When regulating the radio spectrum, it is furthermore necessary to adopt an international outlook. This is of course because radio waves do not stop at national borders, and therefore may end up interfering with or even jamming transmissions of another state [Hook C., 1993]. Therefore, while states will use their sovereign rights to regulate the radio spectrum within their own territory, there are also several levels of international cooperation in order to harmonize spectrum allocation and to ensure effective spectrum management.

At the global level, the radio spectrum is regulated by the ITU for its 193 Member States.[8] At the regional European level, regulation is issued by the European Conference of Postal and Telecommunications Administrations (CEPT) with 48 Member States, including the Russian Federation.[9] At the EU level, the basic provisions regarding radio spectrum management are laid down in the Electronic Communications Code.[10] At the lowest level, states can still adopt their own policies and auction parts of the radio spectrum under their sovereign control. National aspects of spectrum regulation include, *inter alia*, the allocation of frequencies to services, organizing licensing auctions, coordinating with neighbouring countries and international and supranational organizations such as the ITU, CEPT, and the EU.

2.4. Spectrum Regulation at the International Level

2.4.1. International Telecommunication Union

States have a long history of coordinating the facilitation of international communications. In the 19th century, when the telegraph gained

[8] Available at: https://www.itu.int. (accessed: 22.04.2020)

[9] Available at: https://cept.org. (accessed: 22.04.2020)

[10] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L321 of 17December 2018.

popularity, states gathered at the 1865 International Telegraph Convention to discuss international telegraph connections and standardization. This convention resulted in the creation of the International Telegraph Union. States agreed that they would continue to manage telegraphy within their own territory but would let the International Telegraph Union manage international telegraphy. In 1885, the International Telegraph Union also started looking into international telephony. Similarly, when later wireless telegraphy gained popularity, states gathered at the International Radiotelegraph Convention in 1906 and established the International Radiotelegraph Union. As can be determined from its name, this organization concerned the international management of radiocommunications. In 1932, these organizations merged to form a single international telecommunication organization, the International Telecommunication Union (ITU). In 1947, the ITU became a specialized agency of the United Nations (UN), headquartered in Geneva, thus operating within the broader UN framework and network.

Membership with voting rights to the ITU is open to all UN Member States. Additionally, any private organization — such as device manufacturers, service providers, or research institutions — can obtain non-voting membership. The ITU also maintains regional and area offices all over the world and works closely with regional institutions, such as the CEPT. In 1992, the ITU was restructured along three sectors: ITU-R for radiocommunication, ITU-T for standardization, and ITU-D for development. Additionally, ITU Telecom organizes global events.

The goal of ITU-R is "to ensure rational, equitable, efficient and economical use of the radio-frequency spectrum by all radio communication services, including those using satellite orbits, and to carry out studies and adopt recommendations on radio communication matters".11 Apart from the ITU Constitution and ITU Convention the main legal instrument regulating the radio spectrum are the Radio Regulations.[12] This administrative instrument is binding for ITU members.

2.4.2. Radio Regulations

The Radio Regulations are adopted at the World Radio communication Conferences (WRC). These conferences are held in principle every

[11] Available at: www.itu.int/en/ITU-R/information/Pages/mission-statement.aspx. (accessed: 22.04. 2020)

[12] International Telecommunication Union. Radio Regulations. 2016.

four years.[13] The Radio Regulations distinguish between allocation, allotment, and assignment of radio spectrum. Allocation refers to the division of the radio spectrum into frequency bands. This division is laid down in the Table of Frequency Allocations. Allotment means designating a certain frequency band to a category of radio communication services. The allotment can be for one or more identified countries or geographical areas, and under specific conditions. This means that the allotment of frequencies is not necessarily uniform for the whole world but can differ per region in order to cater to regional needs. Assignment means that an administration — typically at the national level — provides authorization to an entity to use a specific frequency channel under certain conditions. Member States must "limit the number of frequencies and the spectrum used to the minimum essential to provide in a satisfactory manner the necessary services" (article 4(1) Radio Regulations). New assignments must avoid interference with frequencies already assigned according to the Table of Frequency Allocations (article 4(3) Radio Regulations). Member States may, however, conclude special arrangements between each other "regarding the sub-allocation of bands of frequencies to the appropriate services of the participating countries" (article 6 (1) Radio Regulations).

2.4.3. The Role of the CEPT

At a Pan-European level, the European Conference of Postal and Telecommunications Administrations (CEPT) was established in 1959. The main goal of the CEPT is to "collaborate to harmonise telecommunication, radio spectrum, and postal regulations to improve efficiency and co-ordination for the benefit of European society".[14] Initially, the CEPT served as the coordinating body for the national telecommunications and postal state monopolists. However, as these entities gradually became privatized during the 1990s, they have been replaced by the competent policymakers and regulators. As of 2020, CEPT has 48 members, including all EU and EFTA nations, the Balkan countries, the Russian Federation, and Turkey. Within the CEPT, the Electronic Communications Committee (ECC) develops common policies and regulations in electronic communications for Europe and is a focal point for information on spectrum use. Its primary objective is to harmonise the efficient use of the radio spectrum, satellite orbits and num-

[13] The most recent World Radiocommunication Conference (WRC-19) took place from 28 October to 22 November 2019 in Sharm el-Sheikh, Egypt.

[14] Available at: www.cept.org/files/1047/CEPT%20Leaflet_June%202018.pdf. (accessed: 22.04.2020)

bering resources across Europe. It also prepares common proposals to represent European interests in the ITU and other international organisations. The ECC itself is supported by Working Groups and Project Teams which carry out expert regulatory and technical studies and consultations to inform the ECC's policy, and to create the deliverables which it approves. Two of the ECC's main outputs are "Decisions" and "Recommendations" on major harmonization issues. Many CEPT Decisions relate to the harmonised use of particular frequency bands for designated functions.[15] CEPT Member States are bound to implement ECC Decisions.

2.5. Spectrum Management Policy of the European Union

2.5.1. EU Radio Spectrum Legislation

In 2002, the EU adopted the Radio Spectrum Decision, calling for coordination on radio spectrum regulation at the level of the EU.[16] The goal of the decision was to facilitate the development of an EU radio spectrum policy — in line with policies adopted at the level of CEPT and ITU — and to ensure effective implementation of radio policy. The decision establishes a Radio Spectrum Committee to advise the European Commission on radio spectrum matters. It also created the Radio Spectrum Policy Group (RSPG).[17] This is a high-level advisory group assisting the Commission in the development of radio spectrum policy, consisting of representatives of the Member States and the European Commission. In doing so, it also takes into account economic, political, cultural, strategic, health, and social considerations, whereas the aforementioned Radio Spectrum Committee is focused more on the technical aspects of spectrum management.

In 2007, the European Commission addressed new market evolutions — such as the growing need for broadband Internet. It therefore proposed amendments to the 2002 framework, which was eventually adopted as the new Telecoms Package in 2009. This package consisted of three texts:

[15] See, for example, the ECC Decision of 13 March 2009 on the harmonised use of the 63.72-65.88 GHz frequency band for Intelligent Transport Systems (ITS), amended on 4 March 2016 and amended on 5 July 2019. Available at: https://www.ecodocdb.dk/download/09d84da1-2776/ECCDEC0901.PDF. (accessed: 22.04.2020)

[16] Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community. OJ L 108 of 24 April 2002.

[17] Commission Decision 2002/622/EC of 26 July 2002 establishing a Radio Spectrum Policy Group. *OJ* L 198 of 27 July 2002.

a directive amending the Framework, Authorization and Access directives;

a directive amending the Universal Services and E-privacy directives; and

a regulation establishing the Body of European Regulators for Electronic Communications (BEREC).

BEREC, based in Riga, serves as the regulating agency for the telecommunications market in the EU. In this capacity, it advises the European Commission on its telecommunications policies. Its board is composed of representatives of the competent national regulators. BEREC replaces the European Regulators Group for electronic communications networks and services, which was established for similar purposes in 2002.

The 2009 amendments mainly concerned measures to strengthen the internal market, to allow for more flexible management of the radio spectrum, to strengthen consumer protection — including the adoption of net neutrality rules. The package also strengthened the role of the European Commission in relation to national market regulators.

In 2016, the European Commission launched the so-called Connectivity Package. As part of this package, it proposed a single European Electronic Communications Code (EU ECC) holding the EU-wide rules on the regulation of the telecommunications market (European Commission, 2016). Other aspects of the package include common broadband targets for 2015, a 5G Action Plan, and a voucher scheme to offer free Wi-Fi access to citizens.[18]

The European Electronic Communications Code was adopted in 2018.[19] It reaffirms that Member States may not prevent an undertaking from providing electronic communications networks or services, unless necessary (article 12(1]), although notification requirements can be implemented, as well as certain conditions (article 13(1)).

Undertakings derive a minimum of rights from the principle of general authorization, such as the right to provide electronic communications services and to use the radio spectrum in doing so (article 15(1)). They may, however, be subjected to administrative charges (article 16(1)). When existing rights get restricted or withdrawn, due compensation is needed (article 19(1)).

[18] Available at: https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access. (accessed: 22.04.2020)

[19] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321 of 17 December 2018.

Member States will continue to coordinate their radio spectrum use, to avoid harmful cross-border interference (article 28(1)). A peer review process is established for when Member States undertake a selection procedure (article 35(2)). In the case of a harmonized spectrum band, when access conditions and procedures have been imposed, and undertakings to which the radio frequencies spectrum was assigned have been selected in accordance with applicable rules, Member States must grant the right of use for such radio frequencies spectrum in accordance with those rules (article 36). Fees can be levied for the right to use the radio spectrum (article 42(1)).

Member States will still ensure access to the radio spectrum in accordance with objective, transparent, procompetitive, non-discriminatory, and proportionate criteria, as well as in respect of international agreements (Article 45(1)). Still, the EU legislator remains principally neutral toward the type of services provided or the technology used (Article 45(4)-(5)). While general authorization remains the basic principle, Member States can still resort to limited or individual authorizations in certain cases (article 46(1)). The use of the spectrum may be subjected to conditions (article 47(1)). Individual rights must be awarded for a certain period of time, ensuring "regulatory predictability for the right holders over a period of at least 20 years regarding investment conditions in infrastructure which relies on the use of such radio spectrum" (article 49(1)-(2)). Individual rights can be renewed (article 50(1)) or transferred and leased (article 51(1)).

The EU-ECC also coordinates the timing for the assignment of the 5G bands, making the 3.4-3.8 GHz and the 24.25-27.5 GHz frequency bands available by the end of 2020 (Article 53a (1)). Where needed, Member States can limit the number of rights granted to part of the spectrum by means of a competitive or comparative selection procedure, "giving due weight to the need to fulfil national and internal market objectives" (Article 54(1) & 54(2)).

2.5.2. EU Radio Spectrum Policy Programme

Apart from the legal framework in the strict sense, the EU has adopted a Radio Spectrum Policy Programme (RSPP) in 2012.[20] The goal of the RSPP

[20] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme, *OJ* L 81 of 21 March 2012.

is to provide a roadmap for the development of the internal market for wireless technologies and services. Regulatory principles, policy objectives, and priorities can all be found in the program, which aims to enhance efficient and flexible spectrum use, in order to strengthen competition within that market.

The EU also recognizes that additional spectrum might be needed by sectors such as transport research and development (R&D), as well as the need to ensure adequate protection against harmful interference to sustain R&D and scientific activities (recital 29 RSPP). It further states that "Member States and the Commission shall collaborate with the scientific and academic community to identify a number of research and development initiatives and innovative applications that may have a major socio-economic impact and/or potential for investment and consider the spectrum needs of such applications and, where necessary, consider the allocation of sufficient spectrum to such applications under harmonised technical conditions and with the least onerous administrative burden" (article 8 RSPP).

A number of actions taken under this program include:

the identification of 1200 MHz of spectrum for increasing wireless data traffic demands;

allowing spectrum trading throughout the EU in harmonized bands;

fostering different modes of spectrum sharing in the EU;

analysing the efficiency of spectrum use in the 400 MHz — 6 GHz range.

Furthermore, Member States must authorize certain bands that have been reallocated for high speed electronic communications services, more precisely the harmonized 900-1800 MHz, 2.5-2.69 GHz, and 3.4-3.8 GHz bands, as well as the 800 MHz band to cover sparsely populated areas.

2.6. National Spectrum Management

2.6.1. National Competences

While many aspects of spectrum regulation are regulated at the international, regional, or supranational level, national governments and regulators still have significant competences in this matter and thus remain the main regulator of the radio spectrum. As part of this work, national authorities will have to develop a national allocation table. While a sovereign state is in principle not bound to follow the ITU's regional allocation table exactly, it is of course wise to do so in order to ensure maximal har-

monization and minimal interference. Moreover, in doing so the national allocation table translates the international and regional allocations into national law.

The national authorities will also determine how to regulate the use of the spectrum. Here, several options are available. In broad strokes, these can be divided between general authorizations and individual authorizations.[21]

In a general authorization, use of the spectrum — or at least of certain bands of the spectrum — will principally be exempt from licensing. This means that in principle no individual license must be obtained in order to use (part of) the radio spectrum. Use of this (part of) the spectrum must therefore also not be notified. This is a model that is often used for consumer-grade devices, such as mobile phones, short-range devices, and amateur radio. Nevertheless, certain rules may still apply, for instance regarding device standards. A particular band may also be designated as a common, meaning that in principle every user and every device can use this band [Medeisis, 2011]. Also here, some general rules may apply, for instance to contain possible interference. For authorities, this model limits their administrative overhead, and the need for coordinating the use of the radio spectrum. For individuals and industry, this model allows for easy and cheap deployment of radio-frequency devices. The main drawback is of course that this may result in uncontrolled use of (that part of) the spectrum, leading to unmanageable interference.

At the other end of the spectrum, there are individual authorizations. Here, use of (part of) the radio spectrum becomes reserved exclusively to those that obtained an individual license. Licenses are generally non-transferable, and subject to regular — generally annual — renewal. Moreover, such licenses are generally subject to fees, to cover the costs incurred by authorities. The main benefit of this model is that it provides the highest degree of security and protection against harmful interference. However, this of course limits the use of the radio spectrum for the broader public, and it requires authorities to organize a — often administratively complex and costly — licensing procedure. There are different ways to grant a license.

One model used in Europe, and particularly in the telecom sector, is that of the auction. In an auction, the competent authority will allow for competitive bidding to gain a license, and only the highest bidder will re-

[21] ECC (2009) *Light licensing, license-exempt and commons*. Available at: https://www.ecodocdb.dk/download/87ccb237-fa9a/ECCREP132.PDF (accessed: 22.04.2020).

ceive a license for the auctioned part of the spectrum [Cave E., Nichols R., 2017]. While bidding is in principle open, authorities can set minimum requirements with which interested entities need to comply. The main benefit of this is that it is a fairly simple mechanism, with the propensity of being beneficial for the treasury. While an auction does principally operate in a free market, it is clear that only the larger and wealthier companies can afford such bid. While this model therefore in principle leaves the matter open to the market, it could also be argued that it enables those with a dominant market position to further entrench themselves [Beltrán F., 2016].

Licenses can also be awarded on a 'first come, first served' basis. In this case, frequencies are awarded in order of application, subject to availability. While this is an oft-used model, there are a few drawbacks. For one, this model only works if the frequencies involved are not too scarce. Moreover, there is little certainty that the entity to which the license is awarded will indeed use that license efficiently. This is, in part, because such model encourages entities to submit an application as early as possible, even if they do not intend to immediately utilize the license.

Other means of awarding licenses include lotteries and beauty contests. The former relies on chance, the latter generally includes a public procurement procedure in which the competent authorities set a number of criteria — possibly with a particular weight attached to each criterion — from which the entity best corresponding to those criteria is selected. Of course, organizing such lottery or beauty contest is a more complicated procedure than that of the auction. In some cases, a more simplified procedure can be envisioned for a more limited number of users, which already leans more to the following model, but still with characteristics of the individual license.

A model in between these options is that of light-licensing. Here, the use of (part of) the radio spectrum is subject to registration. Upon that registration, an interference check is performed to determine whether the intended use would interfere with previous registrations, thus working on a 'first come, first served' basis. Since this process can be fully automated, it requires little to no input from authorities. At the same time, the registration duty allows for the control and limitation of the radio spectrum use and allows for authorities to collect a fee as means of incentive pricing. It is therefore a suitable method for services with a high and fluid demand, such as amateur radio and ship radio licenses.

These models can be summarized as follows.

Table 1

Authorization overview[22]

Individual authorisation (Individual rights of use)		**General authorisation** (No individual rights of use)	
Individual licence	**Light-licensing**		**Licence-exempt**
Individual frequency planning / coordination Traditional procedure for issuing licenses	Individual frequency planning / coordination Simplified procedure compared to traditional procedure for issuing licenses With limitations in the number of users	No individual frequency planning / coordination Registration and/or notification No limitations in the number of users nor need for coordination	No individual frequency planning / coordination No registration nor notification

2.6.2. Spectrum Management in the Russian Federation

In Russia the regulation of the use of the radio frequency spectrum is the exclusive right of the Federal State. The Federal law "On Communication" is the basic legislative act in this domain.[23]

Radio regulations are issued by the State Commission on Frequency Management. A guide published by the State Commission includes the Russian Federation table of frequency allocations in the frequency range 3KHz to 400 GHz, policies on allotment and monitoring of frequency usage, regulations on the production, purchase, import and use of radio equipment, a copy of the legislation relating to wireless and broadcast licensing, information on the certification of radio equipment and a list of the basic EMC standards and technical requirements.

The Government of the Russian Federation establishes the powers of the state executive body, defines the list of radio-electronic means and high-frequency devices, subject to registration, approves a Table of frequency allocations, plans prospective use of radio frequency spectrum, and

[22] ECC (2009) Light licensing, license-exempt and commons. Available at: https://www.ecodocdb.dk/download/87ccb237-fa9a/ECCREP132.PDF (accessed: 22.04.2020)

[23] Federal law of 7 July 2003 (with amendments of 02.07.2021) "On Communication", Art. 22. // SPS CjnsiltantPlus

fixes the charges for use of the radio frequency spectrum, its collection, distribution and use. The Ministry of the Digital Development, Communications and Mass Media of the Russian Federation elaborates the policy, realizes law-making power, appoints a radio frequency or radio frequency channel for radio-electronic means for civil purposes, permits forced changes of a radio frequency or a radio frequency channel in exceptional cases and licenses the provision of electronic communications services.[24]

Licences to use the radio spectrum are issued for a term from three years to 25 years, taking into account the period specified in the application, the nature of the communications service and the period specified by the State Commission for the requested frequency band. In accordance with its Federal laws and Government decrees, the Russian Federation requires a one-time initial payment and an annual fee for use of its radio frequency spectrum.

3. Access to Radio Spectrum for Research Purposes

3.1. Temporary Spectrum Licensing for Testing and Demonstration

Key players in the telecom sector have called upon the European Commission and Member States to "encourage and incentivize cross-sector innovation through adequate policies and support for cross-sector hubs for experiments, trials and large-scale pilot programs". Moreover, in its roadmap for pan-European 5G trials, the 5G Infrastructure Association has called for a specific joint strategy between industry, research centres, academics, local communities, public authorities and domain-specific initiatives (5G Infrastructure Organization, 2016). Experimental hubs, trials and pilots usually work with radio spectrum obtained on a temporary basis for testing and demonstration on a particular location. Procedures for granting such temporary licenses for testing and demonstrations exist in most countries.

In France, for example, applications for radio spectrum for experimental use must be addressed to the Autorité de Régulation des Communications électroniques et des Postes (Arcep).[25] Experimental use in this context is the use of the radio spectrum for the technical or commercial development of a novel technology or service whereby the turnover and number of users

[24] Order of the President of RF of 5 May 2018 №215 // SPS ConsiltantPlus.

[25] Article L42-1(IV) of the Code des postes et des communications électroniques.

of that technology or service remain below a certain threshold during the experiment. This threshold has been set at a turnover of EUR 500.000 and a number of users of 2.500 (D406-17-1 Code des Postes et des Communications électroniques). Applications must describe the frequency bands that will be used, the desired and minimal bandwidth, the location and duration of the experiment, and the test set-up. A more detailed technical description will list the technology and service type, the characteristics of any fixed stations used, and the overall technical and operational architecture. Applications may be filed only by legal persons and their representatives. Licenses can be granted for a maximum of two years. The fees owed for the assignment of a temporary license are calculated by means of a complex formula determined by law.[26]

In Germany, the competent authority is the Bundesnetzagentur, with competences over the telecommunications, postal, railway, and energy markets.[27] According to article 55(1) of the German Telecommunications Act, every usage of the radio spectrum requires an assignment by the Bundesnetzagentur.[28] However, individual deviations from the frequency plan may be justified for testing innovative technologies in telecommunications, or in the event of short-term frequency requirements. Article 58(2) of the German Telecommunications Act therefore allows for temporary licenses to be issued. Such temporary licenses, however, may not hinder pre-assigned frequency use. Applications can be submitted through e-mail. Information to be provided includes the contact information of the applicant, a description of the use including its geographical coverage and time of use, information about the devices, the desired frequency and bandwidth, the antenna's used, and a description of the frequency use. Applications can be filed by natural and legal persons. They must be filed at least four weeks before the intended usage. An EUR 130 fee is levied for temporary licenses per channel, with an additional EUR 50 per channel. Temporary licenses can be issued for up to maximum 30 days, subject to possible extension up to three consecutive months.

[26] Décret n°2007-1532 du 24 octobre 2007 relatif aux redevances d'utilisation des fréquences radioélectriques dues par les titulaires d'autorisations d'utilisation de fréquences délivrées par l'Autorité de régulation des communications électroniques et des postes & Arrêté du 24 octobre 2007 portant application du décret n° 2007–1532 du 24 octobre 2007 relatif aux redevances d'utilisation des fréquences radioélectriques dues par les titulaires d'autorisations d'utilisation de fréquences délivrées par l'Autorité de régulation des communications électroniques et des postes.

[27] Available at :https://www.bundesnetzagentur.de. (accessed : 22.04.2020)

[28] Available at : https://www.gesetze-im-internet.de/tkg_2004/. (accessed: 22.04.2020)

In the United Kingdom, non-operational licenses can be obtained to use the radio spectrum to promote the development and trials of innovative uses of the radio spectrum. Such licenses allow for the testing and development of wireless radio equipment, scientific research and experimentation, and for trials and demonstrations of radio apparatus. Commercial or operational usage is not permitted. Furthermore, these licenses are awarded on a non-interference and non-protection basis. Application can be made through a form provided by Ofcom.[29] Ofcom distinguishes between Innovation and Research licenses — used for research, development and testing purposes — and Demonstration and Trial licenses — largely used for demonstrating and testing new equipment.[30] Innovation and Research licenses allow the use of spectrum on a non-commercial, non-permanent basis in order to build innovative spectrum apparatus or equipment, or to undertake academic or scientific research. Such license also covers the testing of equipment for various purposes. It only allows for the use of spectrum at a single location, such as a university, test facility, factory or laboratory. Involvement of the public is not allowed, but certain collaboration and testing work with third parties is permitted insofar this does not constitute an operational service. A Demonstration and Trial license allows for the use of spectrum on a non-commercial, non-permanent basis to trial and demonstrate a new system, radio concept, application or service. The involvement of third parties in trials is allowed, provided that participants are fully informed on the nature of the trial. Demonstration and Trial licenses can only be obtained for new services not fitting within existing license categories. Both licenses can be awarded for a period of up to one year. While renewal is not possible, a new license can be obtained for further research and trials. Applications can be submitted by both legal and natural persons. Applications must provide information on the project's location and time scale, a description of Costs of these licenses are GBP 50 per year and per location for an Innovation and Research license, and GBP 50 per month and per location for a Demonstration and Trial license [Ofcom, 2018].

In Russia**,** the overall mechanism for allocation of radio frequency bands for conducting R&D and testing new technological solutions does not differ much from the general procedures established by the Russian State Committee for Radio Frequencies (SCRF). The Regulation regarding

[29] Available at: www.ofcom.org.uk/__data/assets/pdf_file/0023/80780/application_form_ofw225.pdf. (accessed: 22.04.2020)

[30] Available at: https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/non-operational-licences. (accessed: 22.04.2020)

the State Committee (§ 15) allows the latter to make decisions related to the allocation of a selected radio spectrum band (or bands) for a specific person (individual or legal entity), with the purpose to conduct scientific, research, experimental and design activities, for a period necessary to perform these activities. In principle every individual can apply for such a license, by submitting a standardised form including an explanatory note with details on the purpose of the trial, the requested frequency band, the geographical location, technical specifications on the radio equipment that will be used, etc. The application will be registered by the SCRF administration within one working day.[31] The SCRF Administration processes the application ("preliminary analysis") within 10 working days from the date of its registration (Section 15 of the Procedure for allocating radio frequency bands). Within five working days after the preliminary analysis (i.e. approximately three weeks after the reception of the application), the SCRF sends a letter indicating the need to examine the possibility of using the requested radio frequency band in the indicated region and (or) in the territory of the Russian Federation, with the attached Radio Frequency Application materials to (a) the Ministry of Defence of the Russian Federation, (b) the Federal Service for Supervision in Telecommunications, Information Technologies and Mass Communications ("Roskomnadzor"), (c) the Federal Protection Service of Russia (FSO), for the clearance on allocating the requested radio frequency band(s). A similar letter will also be sent to other federal agencies, if these agencies could be affected by the temporary license (Section 17 of the Procedure for allocating radio frequency bands). These administrations concerned have approximately six weeks (30 working days) to prepare their opinions on the possibility of allocating the requested radio frequency band(s) and send the opinions (on paper or electronically) to the SCRF Administration (Section 21 of the Procedure for allocating radio frequency bands). Based on the received feedback (clearance or refusal), the SCRF Administration, within 10 working days, prepares a draft decision of the SCRF for further approval by the Commission.

If within a term of processing of the Application, the need for additional technical tests (to assess the electromagnetic compatibility etc.) appears, the Commission makes the decision to extend the processing of the application based on the substantiated justification of the concerned member

[31] Processing of the Applications is organized by the SCRF Administration in accordance with the Regulations of the SCRF and the "Procedure for reviewing materials and making decisions on the allocation of radio frequency bands, re-issuing and amending decisions", approved by the Decision of the SCRF of December 20, 2011. No 11-13-01.

of the SCRF. Such extension may be made only once and for the period not more than six months (Section 21 of the Procedure for allocating radio frequency bands).

Decisions of the SCRF are taken by a simple majority of votes of members of the Commission by open vote, taking into account written opinions of members of the Commission. In case of equality of votes (tie), the vote of the Chairperson of the meeting prevails. All decisions are published on the official website of the Ministry of the Telecommunications. Particular decisions on allocation of radio frequencies to a specific person are sent to the applicant in the form of an extract from the Decision of the SCRF.

4. Access to spectrum via spectrum trading or leasing

Temporary spectrum usage licenses for the testing and development of wireless radio equipment, scientific research and experimentation, and for trials and demonstrations of radio apparatus, are typically suited for operating limited testbeds. As already emphasized before, there is currently also a need to test innovative solutions on the large-scale operational networks of the MNOs. Theoretically, this could be solved by granting usage rights in the same frequency band to multiple users, whereby every user makes use of technologies to dynamically share the radio spectrum without mutual interference.

4.1. Access to spectrum via (dynamic) spectrum sharing

Dynamic spectrum sharing techniques have been developed in order to answer the need for better utilization of the spectrum resources. In the following, an overview is provided of the spectrum sharing principles and the regulatory status of different spectrum sharing methods in Europe and USA.

4.1.1. Spectrum sharing overview

Currently, cellular mobile communications networks, such as 2G, 3G and 4G, are typically deployed by a small number of MNOs. These deployments are based on individual access rights that are acquired through auctions organized by national regulatory authorities. Usually, these access rights cover wide geographical areas and are granted for long-term use and give the MNO exclusive access to the spectrum band [Cramton P., 2013]; [Olla P., Patel N., 2002]; [Feasey R., 2015]. On the other hand, the bands that have not been allocated to the mobile communications are usually

licensed for other use, such as TV broadcasting or terrestrial-satellite communications.

As it is challenging to clear spectrum bands from incumbent usage, sharing-based spectrum governance models have become increasingly appealing for NRAs to allow new entrants to use otherwise underutilized spectrum bands in a timely manner [Anker P., 2017]; [Beltran G., 2017]. This has led to the development of spectrum sharing mechanisms where two or more wireless systems operate in the same spectrum band [ITU, 2014; RSPG, 2011; RSPG, 2013]; [Matinmikko-Blue M., 2018]. Spectrum sharing methods can be categorized according to licensing and authorization into individual authorization, light licensing and license-exempt access.

The currently dominating spectrum licensing scheme is dedicated access, one of the individual authorization methods. In individual authorization the MNO, or another spectrum user such as a satellite system, is granted an exclusive right to utilize the spectrum band. Co-primary shared access falls also under individual authorization. Under this scheme, the license holders use their licenced spectrum jointly in a shared manner through mutual agreements, subject to the permission of the competent authority. The participating MNOs have equal access rights to the spectrum, without priorities set by the authority.

Licensed shared access (LSA) and authorized shared access (ASA) also belong under the individual authorization regime. Although ASA and LSA essentially refer to same paradigm, ASA can be seen as a special case of LSA where the licensee is an MNO, while in LSA the licensee can also be another type of entity. However, in both ASA and LSA, a non-mobile communication license holder, referred to as incumbent, can share spectrum with one or more mobile communications systems under certain rules and in non-interfering basis.

The term light licensing refers to a simplified and more flexible regulatory framework of issuing spectrum authorizations compared to fully exclusive authorization, usually targeted to the frequency bands where the risk of interference is low [Dahlberg C. et al., 2013]. Example target bands considered reasonable for this access method are 60 GHz and 80 GHz bands, whose propagation characteristics facilitate the use with minimum risk of interference.

License-exempt access or unlicensed access refers to a scheme where a set of users co-exist and are able to utilize a specific frequency bands opportunistically with equal priority rights. The bands can range from li-

censed to unlicensed bands such as narrowband licensed television white space (TVWS) and Wi-Fi bands in 5 GHz. However, the users operating on this licensing regime must comply with the general technical regulations defined for the bands and be certified.

4.1.2. Regulatory concepts for spectrum sharing

4.1.2.1. Europe: LSA and ASA

LSA was introduced as a general concept to facilitate controlled sharing between any two systems in such way that predictable QoS is provided.[32] The RSPG provided an opinion on this matter in which it defines LSA as "a regulatory approach aiming to facilitate the introduction of radio communication systems operated by a limited number of licensees under an individual licensing regime in a frequency band already assigned or expected to be assigned to one or more incumbent users. Under the Licensed Shared Access (LSA) approach, the additional users are authorised to use the spectrum (or part of the spectrum) in accordance with sharing rules included in their rights of use of spectrum, thereby allowing all the authorized users, including incumbents, to provide a certain Quality of Service (QoS)".[33] LSA is therefore not a new licensing regime, but a complementary spectrum management tool that allows multiple individual licensees to each have exclusive individual access to a portion of spectrum at a given location and time. Harmonized usage conditions would need to ensure a smooth coordination between incumbent licensees and new licensees allowed under the LSA regime.

The first regulatory report from the CEPT on LSA provided an overall description of the LSA concept as a general regulatory framework and its applicability to the current regulatory practices regarding spectrum use.[34] The EU then gave a Mandate to the CEPT to study harmonized conditions for mobile use regarding the 2.3–2.4 GHz band. As a response, the guidelines for the sharing framework for LSA for this band were developed by the CEPT.[35] First, regulatory and technological options for sharing be-

[32] RSPG (2011). Report on collective use of spectrum (CUS) and other sharing approaches.

[33] RSPG (2013). Opinion on licensed shared access. RSPG13-538.

[34] ECC. Report 205: Licensed Shared Access (LSA). Available at: https://www.ecodocdb.dk/download/baa4087d-e404/ECCREP205.PDF (accessed: 22.04.2020)

[35] ECC. Decision (14) 02: Harmonized technical and regulatory conditions for the use of the band 2300-2400 MHz for Mobile/Fixed Communications Networks (MFCN).

tween mobile broadband and the relevant incumbent services were identified. This included an overview of different incumbent services on the band in all European countries and options for sharing for each of these services.[36] The incumbent services are Programme Making and Special Events (PMSE), telemetry, fixed links, and Unmanned Aircraft Systems (UAS). There is also an amateur service on a secondary basis, but it does not need to be protected in the same way as other incumbent services. Second, a more detailed study on the technical sharing solutions between the mobile broadband and PMSE was given.[37] In this study, a step-by-step approach for the implementation of an LSA sharing framework was introduced with the following steps: determining the extent and type of incumbent use, calculating the protection criteria for the incumbent, and identifying operational conditions for sharing, such as implications for the mobile network.

Shared use of the radio spectrum has also been included in the EU-ECC, which specifically mentions the possibility of LSA (Article 2 (26) EU-ECC). Articles 45(2) and 46 of the EU-ECC require Member States to promote and set the conditions for the shared use of the radio spectrum, in accordance with competition law.

4.1.2.2. European TV white spaces

Television white space (TVWS) equipment operates in the unused frequency gaps between high power television broadcast stations The European regulatory activities on TVWSs were initiated in the ECC of CEPT by addressing technical and operational requirements for the possible operation of cognitive radio systems in the white spaces in order to protect the incumbent radio services from the harmful interference.[38] The work was

https://www.ecodocdb.dk/download/b02d6dab-2b58/ECCDEC1402.PDF (accessed: 22.04.2020)

[36] CEPT (2015) Report 56: Technological and regulatory options facilitating sharing between wireless broadband applications (WBB) and the relevant incumbent services/applications in the 2.3 GHz band. Available at: https://www.ecodocdb.dk/download/16fde9f8-9f82/CEPTREP056.PDF. (accessed: 22.04.2020)

[37] CEPT (2015) Report 58: Technical sharing solutions for the shared use of the 2300–2400 MHz band for WBB and PMSE. https://www.ecodocdb.dk/document/related/58. (accessed: 22.04.2020)

[38] ECC (2011) Report 159: Technical and operational requirements for the possible operation of cognitive radio systems in the white spaces of the frequency band 470-790 MHz. Available at: https://www.ecodocdb.dk/download/be051b35-91e9/ECCREP159.PDF (accessed: 22.04.2020)

continued with technical investigations for the development of the regulation for white space devices.[39] Next, the use of centralized geo-location databases for protection of the incumbent services, including framework proposals and feasibility assessment, was provided.[40] Finally, ECC introduced the overall framework for TVWS devices using geolocation databases and for providing guidance for national implementation, including options for database policy and provision.[41]

4.2. European regulatory framework for spectrum sharing

4.2.1. EU Telecommunications framework

As noted before, the European legislator in the 2009 overhaul of its telecoms package decided to open up the possibility for a secondary radio spectrum market to develop. This was the result of the insertion of a new provision, Article 9b, by the so-called Better Regulation Directive[42] into the former Framework Directive.[43]

The Article 9b of the amended Framework Directive allowed for the transfer or lease of individual rights to use radio frequencies. It established the basic principle that Member States must allow undertakings to transfer or lease to other undertakings their individual rights to use radio frequencies. Such transfer must be in accordance with the conditions attached to

[39] ECC (2013) Report 185: Complementary Report to ECC Report 159. Further definition of technical and operational requirements for the operation of white space devices in the band 470-790 MHz. https://www.ecodocdb.dk/document/related/292 (accessed: 22.04.2020)

[40] ECC (2013) Report 186: Technical and operational requirements for the operation of white space devices under geo-location approach. European Conference of Postal and Telecommunications Administrations. Available at: https://www.ecodocdb.dk/document/293 (accessed: 22.04.2020)

[41] ECC (2015) Report 236: Guidance for national implementation of a regulatory framework for TV WSD using geo-location databases. Available at: https://www.ecodocdb.dk/document/related/342 (accessed: 22.04. 2020)

[42] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337 of 18 December 2009.

[43] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108 of 24 April 2002.

their rights of use of radio frequencies and in accordance with national procedures.

Moreover, the amendment allowed transfers within the bands for which this is provided by the implementing measures adopted by the European Commission, which did not cover frequencies used for broadcasting. Member States could allow undertakings to transfer or lease their individual rights to use radio frequencies in other bands as well, in accordance with national procedures.

Any conditions that were imposed on individual right holders to use radio frequencies continued to apply after the transfer or lease, unless otherwise specified by the competent national authority. A waiver to this could be granted by the Member States for the cases where the undertaking's individual right to use radio frequencies was initially obtained free of charge.

Any undertaking's intention to transfer its rights to use radio frequencies, as well as the effective transfer thereof, had to be notified in accordance with national procedures to the competent national authority responsible for granting individual rights of use, and be made public. Where a harmonization of radio frequency use was involved, any transfer had to comply with that harmonized use.

4.2.2. EU-ECC

The EU Electronic Communications Code (EU-ECC) adopted in 2018 maintains the principles of the previous provision in its Article 51, albeit in a somewhat altered form.[44] The EU-ECC states that Member States must ensure that undertakings may transfer or lease to other undertakings their individual rights of use for radio spectrum. In such case, the original conditions attached to the rights of use are maintained. They may still allow a waiver of the procedure where the undertaking's individual right to use radio spectrum was initially obtained free of charge or assigned for broadcasting.

An undertaking's intention to transfer or lease rights of use for radio spectrum, as well as the effective transfer thereof, must still be notified in accordance with national procedures to the competent authority, and be

[44] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321 of 17 December 2018.

made public. Also here, when there is harmonization, any transfer must comply with such harmonized use.

New in the EU-ECC is that, to prevent a distortion of competition, Member States must submit transfers and leases to the least onerous procedure possible. They may not refuse the lease of rights of use for radio spectrum where the lessor undertakes to remain liable for meeting the original conditions attached to the rights of use, and they may not refuse the transfer of rights of use for radio spectrum unless there is a clear risk that the new holder is unable to meet the original conditions for the right of use. However, this does not diminish the competence of Member States to enforce compliance with the conditions attached to the rights of use at any time, both with regard to the lessor and the lessee, and in accordance with national law.

The transfer or lease of rights of use for radio spectrum must be facilitated by competent authorities by giving timely consideration to any request to adapt the conditions attached to the right, and by ensuring that the rights or the radio spectrum attached thereto may to the best extent be partitioned or disaggregated. Administrative charges imposed on undertakings in connection to processing an application for the transfer or lease of rights of use for radio spectrum may only cover the administrative costs incurred in the management, control, and enforcement of the authorization scheme.

Relevant details relating to tradable individual rights must be made publicly available in a standardized electronic format when the rights are created and must be maintained as long as the rights exist. The European Commission can adopt implementing measures to identify such relevant details.

4.2.3. Implementation of trading and leasing

4.2.3.1. Implementing measures

The goal of the European legislator is to facilitate flexibility and efficiency on the spectrum market, and to allow spectrum valuation by the market.[45] Such would need to lead to more effective spectrum use, while

[45] Recital 132 of the EU Electronic Communications Code: "Transfer of rights of use for radio spectrum can be an effective means of increasing the efficient use of spectrum. For the sake of flexibility and efficiency, and to allow valuation of radio spectrum by the market, Member States should by default allow radio spectrum users to transfer or lease

still allowing national regulatory authorities to take action in preventing a distortion of competition where spectrum is left unused.

In 2011, the ECC published a report on the spectrum trading practices of CEPT countries.[46] At the time, a significant discrepancy between EU Member States was found regarding the possibilities for trading or leasing radio spectrum rights of use. This discrepancy can be explained in the sense that several Member States were still busy transposing the 2009 overhaul of the EU telecoms package.

The implementing measures referenced in the amended Framework Directive were adopted as part of the aforementioned Radio Spectrum Policy Programme.[47] The RSPP determines that Member States must apply technology and service neutrality in the rights of use of radio spectrum for electronic communications networks and services and the transfer or lease of individual rights of use of radio frequencies (article 2(2) (a) RSPP).

More importantly, it is determined that Member States must allow the transfer or leasing of rights of use of spectrum in the harmonized bands of 790-862 MHz, 880-915 MHz, 925-960 MHz, 1710-1785 MHz, 1805-1880 MHz, 1900-1980 MHz, 2010-2025 MHz, 2110-2170 MHz, 2.5-2.69 GHz, and 3.4-3.8 GHz (article 6(8) RSPP). A later decision added that, when granting rights of use in the 470-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services, Member States must allow the transfer or leasing of such rights in accordance with open and transparent procedures pursuant to the applicable Union law (article 2 Decision (EU) 2017/899).[48]

The RSPP was to be applied by the Member States by 1 July 2015. As a result, trading or leasing rights of use in the harmonized bands mentioned in the previous paragraph should now be possible across the EU. Individual Member States may additionally allow transferring or leasing in other

---

their rights of use for radio spectrum to third parties following a simple procedure and subject to the conditions attached to such rights and to competition rules, under the supervision of the national regulatory authorities responsible."

[46] ECC (2011a) Report on the description of practices relative to trading of spectrum rights of use. Available at: https://www.ecodocdb.dk/download/0e2afea8-17cc/ECCREP169.PDF (accessed: 22.04.2020)

[47] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme, OJ L 81 of 21 March 2012.

[48] Decision (EU) 2017/899 of the European Parliament and of the Council of 17 May 2017 on the use of the 470-790 MHz frequency band in the Union, OJ L 138 of 25 May 2017.

bands as well. National provisions must be brought in line with Article 51 of the EU-ECC by 21 December 2020.[49]

4.2.3.2. Distinction between trading and leasing

The notions of trading and leasing are not defined in the European legislation. Nevertheless, a number of observations can be formulated.

Trading of rights of use involves the transfer of spectrum usage rights — and accompanying obligations — from one right holder to another party. In this case, that other party is granted a license by the competent authority to use spectrum following a commercial transaction with an existing license holder involving the transfer of the license rights and obligations.[50] Trading can involve a partial or full transfer of the right holder's radio spectrum usage rights. In case of a full transfer, the accompanying obligations will be fully transferred to the recipient as well. In case of a partial transfer, both the original right holder as the recipient can be bound to the same obligations in the exercise of their respective rights. When rights are traded, their transfer is considered definitive and they do not revert back to the original right holder.[51]

Leasing, in turn, requires a contract allowing one party to exploit the rights of use of a right holder for a certain — usually limited — period of time. However, the original rightsholder maintains its license — and all rights and obligations that go with it. In such case, the right holder can exercise certain control over the party to which usage rights are leased. The leaseholder, however, does not in any way receive a license in its own right. When the lease expires, all rights revert back to the original right holder.

4.3. National legal frameworks for spectrum sharing

How did the EU Member States transpose the aforementioned provisions of European law regarding trading of spectrum usage rights? In this article we will only refer to some examples.

[49] Article 124 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321 of 17 December 2018.

[50] ECC (2011aReport on the description of practices relative to trading of spectrum rights of use. https://www.ecodocdb.dk/download/0e2afea8-17cc/ECCREP169.PDF. (accessed:22.04.2020).

[51] Ofcom (2011) Simplifying Spectrum Trading Spectrum leasing and other market enhancements. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0030/62778/statement-spectrum-leasing.pdf. (accessed: 22.04. 2020)

In France, Article L42-3 of the Post and Electronic Communications Code[52] determines that the French Government can decide upon the frequencies in which licenses can be transferred. All intended transfers must be notified to Arcep, which will make those notifications public. When a frequency has been individually assigned or is used for the exercise of public services, the transfer is subject to prior approval by Arcep. Article R20-44-9-1 of the Code confirms that licensed frequency can be transferred entirely or partially. Article R20-44-9-2 reiterates the principle that individually assigned frequencies can only be transferred upon prior approval by Arcep. Other transfer intentions are only notified to the authority, which can oppose them. Article R20-44-9-3 provides that a request to Arcep must be filed jointly by the original right holder and the recipient. In the case of leasing, the notification must also include elements to guarantee the continuity of the public service missions for which the license to use frequencies is used, and details on how both parties aim to meet the obligations arising from the commitments resulting from their license.

Article R20-44-9-4 provides that a transfer involves the transfer of all rights and obligations relating to the usage right to the recipient. Both the original right holder and the recipient pay the fees for the rights they respectively hold at the end of the transfer. Some of the rights, however, must be divided proportionately. Article R20-44-9-5 provides that Arcep may only oppose a transfer if the general rules for obtaining a license are not met, if the rules for the transfer are not complied with, if there is a danger to effective competition on the market, if there is a non-compliance with the conditions set, or if a sanctions procedure has opened against one of the parties. Article R20-44-9-6 provides that Arcep may impose conditions to ensure compliance with earlier stipulated license conditions. Such conditions may relate to the use of the frequencies or frequency bands involved, or to the distribution of commitments made, if any, in the context of the license procedure. Article R20-44-9-7 adds that Arcep has six weeks to make its decision on the transfer. If the transfer is agreed upon, the original license must be revoked, and a new license must be issued to the recipient of the transfer.

Article R20-44-9-8 concerns leasing. Here, Arcep has three months to make its decision. Article R20-44-9-9 allows this period to be extended if there are reasons for a more thorough examination.

Article R20-44-9-10 provides that any transfer, together with Arcep's decision, must be made public. The National Frequency Agency will up-

[52] Code des postes et des communications électroniques. Available at : https://www.legifrance.gouv.fr. (accessed: 22.04.2020)

date the frequency plan. Article R20-44-9-11 allows that the recipient requests to obtain the rights in absence of a response by Arcep. Article R20-44-9-12 defines what information must be included in the public register of licenses.

In Germany, Article 55(8) of the German Telecommunications Act provides that a transfer of usage rights must be notified to the *Bundesnetzagentur* by submitting in writing a request thereto. The frequencies may continue to be used until a decision is taken. If all requirements for the use of radio spectrum are met, if there are no competition issues, and if there are no interference risks, the transfer should be approved. Article 62 of the same act provides that the *Bundesnetzagentur* can assign additional frequencies allowing trading.[53]

In the UK, Section 30 of the 2006 Wireless Telegraphy Act regulates spectrum trading.[54] It provides that Ofcom may authorize transfers of spectrum licenses. Transfers under bands identified in the RSPP should be authorized. Both the original rightsholder and the recipient are to some extent bound to compliance with the terms of the license and the transfer. Partial transfers can be allowed, be it that regulations may restrict certain factors and that also here authorization by Ofcom is required. Upon transfer, the original license is surrendered and a new one is issued to the recipient. Ofcom may impose conditions on the transfer and may determine the procedure for the transfer. Time-limited transfers are also possible. Leasing is only possible if the license explicitly permits so, but where permitted does not require prior authorization by Ofcom.

The Wireless Telegraphy (Mobile Spectrum Trading) Regulations 2011[55] provide that complete transfers are allowed when the rights and obligations of the original rightsholder become the exclusive rights and obligations of the recipient, or when the transferred rights and obligations become rights and obligations of the recipient while continuing, concurrently, to be rights and obligations of the original right holder. Partial transfers are also possible in those cases, if the transfer relates to part of the frequency range, part of the geographical scope of the license, or both.

[53] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist (TKG).

[54] Wireless Telegraphy Act 2006, amended by the Electronic Communications and Wireless Telegraphy Regulations 2011. Available at: http://www.legislation.gov.uk/ukpga/2006/36/contents (accessed: 22.04.2020)

[55] Available at: http://www.legislation.gov.uk/uksi/2011/1507/made (accessed: 22.04.2020)

Transfers are not allowed when not all parties consent thereto, when there are still fees to Ofcom outstanding, when the license has been revoked, when a license revocation request has been filed, or when Ofcom does not consent to the transfer.

Procedurally, the notification to Ofcom must identify both parties to the transfer, the license number, whether it is a full or partial transfer, the transfer agreement, and all other necessary information regarding the transfer or rights and obligations. Ofcom will publish that it has been notified and decide on the matter. Ofcom can authorize the transfer or give additional directions. Those directions can make the transfer conditional subject to compliance with certain requirements. Ofcom will take into account whether the rights and obligations of the license are met by the original right holder, whether the recipient can meet those obligations, whether competition will be distorted, or whether there are matters of national security or international arrangements at stake. Following its authorization, Ofcom will issue a new license to the recipient and revoke the original license. The decision will be made public.

An overview of license trades can be found in Ofcom's Spectrum Information Portal.[56]

In the Russian Federation, since the overall legal nature of the radio spectrum is not fully clear in the codified Russian laws (e.g. Civil Code of the Russian Federation), the possibility of "leasing" spectrum does not exist. The permission for the use of frequencies always indicates the entity (or person) responsible for using the allocated frequency band. In case of any troubles/violations, the regulatory body will communicate with this entity only. The participation of any third party is not considered. As already mentioned, the purpose of using certain frequencies should be indicated in the application. If a commercial organization intends to use frequencies for commercial purposes, then transferring permission to another person for non-commercial (research) use is impossible. However, if a frequency sharing scheme is already being introduced, when submitting an application, the applicant agrees in advance with the possibility of using the same frequencies by third parties in agreement with them. This began to happen often by agreement between mobile operators in different regions of Russia, in which one of them has a spectrum deficit. However, the purpose of using the spectrum must remain the same.

[56] Available at: https://www.ofcom.org.uk/spectrum/information/spectrum-information-system-sis/spectrum-information-portal (accessed: 22.04.2020)

Conclusion

In our study, it was found that all EU Member States offer the possibility to obtain a license for the use of radio spectrum for research, testing, and experimental purposes. However, as this is not an EU-harmonized matter, the procedures, requirements, and costs for obtaining such license vary significantly. Also, the duration of these licenses varies greatly, going from just a few weeks in some Member States to several years — including potential renewals — in others, with the average being up to one year. Also, there is no procedure to obtain a license for cross-border testing and experimental purposes. As a result, when a test or experiment would span several Member States, licenses would have to be obtained in each of those states. However, given the lack of coordination in this matter, there is also no guarantee that licenses in the same frequency bands can be obtained in such cross-border settings.

With regard to the primary frequency market, the main finding is therefore that it is principally possible to obtain licenses for research, testing, and experimental purposes in all EU Member States, including in the current 3G and 4G bands. However, given that such licenses are generally awarded for a fairly short duration only, and given the lack of coordination in terms of available bands for these purposes at the EU level, the general conclusion is that this method does not allow for the creation of a persistent and pan-European network of wireless capacity for research, testing, and experimental purposes. While most EU Member States do already have tests in 5G bands ongoing, there are no clear indications that this would directly result in the creation of a more permanent research infrastructure within the 5G spectrum.

The question is then whether there are possibilities on the secondary market, *i.e.* by obtaining radio spectrum from a licensed operator either through transfer of license rights and obligations or by renting or leasing part of that operator's spectrum. Here, it is clear that the European legislator has taken the necessary steps to make this possible by requiring Member States to implement procedures for license transfers and leases, within a number of frequency bands defined in the RSPP. In this field, there is therefore at least a certain baseline of harmonization, although the precise procedures can still vary between Member States. Overall, it was found that Member States require prior notification of the intended transfer or lease to the competent authority. This authority will generally do a number of checks, mainly to verify that licensing requirements are complied with and that the transfer or lease does not disturb competition on the market.

If everything is found correct, the authority will authorize the transfer or lease. Only in one Member State it was found that the competent authority must only be notified but does not have to give prior authorization. Overall, the procedures for this were found to be fairly similar across the board.

Can transfers or leases then provide a solution to the spectrum needs of the research community? Leases offer the benefit that they are easier to obtain in the sense that the license rights and obligations principally remain with the original right holder. The recipient will only receive the right to use part of the right holder's spectrum, under the conditions set by the lease. This allows, for instance, for agreements to be made on the placing of base stations. While leases are considered as being of limited duration, there do not seem to be explicit maximum durations, be it that the lease can of course not outlast the license itself. It can therefore provide a more durable solution than the short-term licenses for research, tests, or experiments found on the primary market. Transfers would of course make for an even more persistent solution, as here all rights and obligations are transferred for the complete duration of the license. However, such transfer also implies that the recipient of the transfer must comply with all license requirements, which in some Member States requires the presence of a legal person registered as an operator.

Briefly summarizing, the necessary European level regulation exists that would allow for example LSA type of flexible spectrum management to be applied between researchers and commercial mobile network operators (MNOs). In addition, standardised technical specifications exist in 3GPP for implementing the LSA in the way that they have been specified by the regulatory authorities. The remaining obstacle is the weak position of researchers and research institutions to enter into the negotiation and conclusion of agreements with MNO's. One of the possible remedies is to assign this task to a specialised entity, preferably at the EU level. A study investigating the feasibility to establish such kind of entity is the objective of the Eu Wireless action, funded by the European Commission under the Horizon 2020 programme. In addition, political support, for example in the form of an EU Recommendation, to overcome the reluctance of MNOs to share their spectrum usage rights with the research community would be most welcome.

References

1. Anker P. (2017) From spectrum management to spectrum governance. *Telecommunications Policy*, vol. 41, pp. 486–497.

2. Beltrán F. (2016) *A Review of the Evolution of Auctions As a Method for Radio Spectrum Assignment*. Available at: http://dx.doi.org/10.2139/ssrn.2828543. (accessed: 22.04 2020)

3. Beltran G. (2017) Accelerating the introduction of spectrum sharing using market-based mechanisms. *IEEE Communications Standards Magazine,* no. 1, pp. 66–72.

4. Berge E., Kranakis E. (2011) Technology-dependent commons: the radio spectrum. *International Journal of the Commons*, pp. 86–91.

5. Brito J. (2006) The Spectrum Commons in Theory and Practice. *Stanford Technology Law Review*.

6. Cave M., Nichols R. (2017) The use of spectrum auctions to attain multiple objectives: Policy implications. *Telecommunications Policy,* no. 5–6, pp. 367–378.

7. Coase R.H. (1959) The Federal Communications Commission. *The Journal of Law and Economics*, pp. 1–40.

8. Cramton P. (2013) Spectrum auction design. *Review of Industrial Organization,* vol. 42, pp. 161–190.

9. Dahlberg C. et al. (2013) A techno-economic framework of spectrum combining for indoor capacity provisioning. In: *Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun.* London: IEEE, pp. 2759–2763.

10. Donovan J. (2019) *How Do Wireless Networks Transmit Data*. Available at: https://blog.commscopetraining.com/how-do-wireless-networks-transmit-data. (accessed: 22.04. 2020)

11. Ellingson S.W. (2016) *Radio Systems Engineering*. Cambridge: Cambridge University Press.

12. Feasey R. (2015) Confusion, denial and danger: The response of the telecommunications industry to the challenge of the Internet. *Telecommunications Policy,* vol. 39, pp. 444–449.

13. Hardin G. (1968) The Tragedy of the Commons. *Science*, vol. 162, No. 3859, pp. 1243–1248.

14. Herter C.A. (1985) The Electromagnetic Spectrum: A Critical Natural Resource. *National Resources Journal*, vol. 25, issue 3. pp. 651–663.

15. Hook S.A. (1993) Allocation of the Radio Spectrum: Is the Sky the Limit? *Indiana International & Comparative Law Review*, vol. 3, pp. 319–360.

16. Martin O. (2012) *The "Hidden" Prehistory of European Research Networking*. Bloomington: Trafford Publishing. 126 p.

17. Matinmikko-Blue M. (2018) *Stakeholder analysis for the development of sharing-based spectrum governance models for mobile communications*. PhD dissertation. University of Oulu.

18. Olla P., Patel N. (2002) A value chain model for mobile data service providers. *Telecommunications Policy,* no. 26, pp. 551–571.

19. Ostrom E. (1990) *Governing the commons: the evolution of institutions for collective action*. Cambridge: Cambridge University Press.

20. Rishabh D. (2016) Governing Spectrum Commons. *TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy*.

21. Samuelson P. (1954) The pure theory of public expenditure. *The Review of Economics and Statistics*, no. 4, pp. 387–389.

22. Shokhin V.D. (2010) Nature and Assignment of the Permission System. *Herald of Moscow State University. Law,* no. 6, pp. 63–64. (In Russ.).

23. Stahov A.I. (2009) Public Administrative Measures for Providing Security. *Zakony Rossii: opyt, analiz, praktika* = Russian Laws: Experience, Analysis, Practice, no. 9, pp. 25–29. (In Russ.).

24. Subanova N.V. (2012) *Permissive Powers of Executive Bodies in Russian Federation.* Moscow: Jurisprudencia, 288 p. (In Russ.).

Information about the authors:

J. Dumortier — Partner, Lawyer.

I.Yu. Bogdanovskaya — Doctor of Sciences (Law), Professor.

N. Vandezande — Legal Consulter.

M.V. Yakushev — Senior Lecturer.

The article was submitted 12.10.2020; approved after reviewing 11.10.2021; accepted for publication 01.11.2021.

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4

Research article
UDC: 342
DOI: 10.17323/2713-2749.2021.4.70.97

Understanding the Algorithm: Meaning, Socio-Legal Context and Concerns

Nabil Ahmad Afifi[1],
Reeta Sony A.L.[2]

[1, 2] Jawaharlal Nehru University, New Delhi, India

[1] nabil58_sse@jnu.ac.in

[2] reetasony@mail.jnu.ac.in

Abstract

At present, algorithms are becoming the heart of society by taking control over the decision-making process as societies are increasingly getting digitalised. There is a consistent theme that an unaccountable, black box technology has taken over the stage and is now making decisions for us, with us, and about us. But the contention around public participation in making decisions in science and technology needs to advance to a stage where there is a more direct conversation between the public and those developing the technologies. With the above mentioned conception of moderating emerging technologies' development, primarily digital technology due to its overreaching effects on humans and what humans interpret it to be. Firstly, the research through a literature survey is aimed to understand the meaning and nuances of the word *algorithm*. Then the analysis based on case study is focused on the algorithmic questions, such as bias, privacy, design, transparency, and accountability. In a larger context, concerns over jobs, ways of social interactions, etc., had been discussed, since these concerns are the result of the application of algorithms. The analysis of academic literature pointed out the vital facet of multiple understanding of the word *algorithm*. Further, the research also emphasizes the meaning of philosophy and politics in technology and its non-neutral nature.

Keywords

algorithms, technology, automated decision-making, algorithmic culture, bias, design

For citation: Afibi N.A., Sony R. A. L. Understanding the Algorithm: Meaning, Socio-Legal Context and Concerns. *Legal Issues in the Digital Age.* 2021, vol. 2, no. 4, pp. 70–97. DOI: 10.17323/2713-2749.2021.4.70.97.

Introduction

The modern world has made quite a shift in functioning, from socio-economic developments to working culture due to the dramatic and drastic digitalization of human life during the Covid-19 pandemic. The digitalisation efforts are changing the very nature of society its approaches to using technologies. Soft technologies[1] have taken centre stage, and algorithms, being the heart of technologies, have intertwined their logic into social interactions and experiences. Thus, it would be safe to say that the thin line of control about humans having agency over technology is diminishing fast. As the world is moving towards the Fifth Industrial Revolution, trying to incorporate a more balanced relationship between intelligent technologies and humans, we stand on the brink of a technological revolution that would shape the future of life, work, and relations. But the widespread propagation of algorithms epitomises a challenge for society and social sciences research.

The all-embracing use of search algorithms, social media, and other digital platforms for browsing, posting, promoting, and advertising has made the human experience more routine. In return, these cyclic activities generate relevant data on user engagement, retention, and research through comments, page views, search ranks, etc., for the corporations owning these technologies. The data collected is integrated on a scale unimaginable for both benefits and unintended consequences [Conger S. et al., 2013]. These practices also foster *cultural production* and *cultural contingent*[2] [Nieborg D.B., Poell T., 2018]. But when culture is numerically sorted, analysed and stored, it becomes crucial to understand that how are these decisions made and how laws and policies are laid out to map, scrutinise, and regulate them.

Law and policy-making are the guardians of digital space to save society from malicious intentions and various concerns that arise due to the usage of digital technology. The law and policy-making both depend on what the diagnosed problem is. To generalise, both law and policy function on stan-

[1] Soft technology should exhibit two main characteristics, i.e., it should be technological and also soft. The technological part includes a knowledge system of rules or procedures for the solution, bringing social or economic change. The Softness part should consist of an internal human conscious activity and affect our understanding of the world.

[2] Contingency in digital platform studies suggest two distinct but interrelated ideas.

dardising definitions of specific terms. This article explores the meaning of the term algorithm, moving beyond the computer science or mathematical description of the term towards social understanding and identifying concerns arising around them.

In order to explore the understanding of the term *algorithm*, authors of the article try to comprehend the meaning through the lens of algorithmic culture. This implies an extensive review of various articles, papers, and books on algorithmic culture and various themes revolving around it. The methods applied in these literature ranges from semantic understanding, etymological to anthropological approaches.

The concerns arising from the digital platforms and software are predominantly the intended or unintended consequence of coding social activities by computational instructions using algorithms. The emphasis in this article is to understand the role law and policy-making had played or could play rather than revolving around definitional and explanatory ideas of the notion of algorithm.

1. *Algorithm* in General Understanding

The study about algorithms is incomplete or, so to say, inaccurate without pondering upon the definition of algorithm. The common understanding of algorithms is more related to computer science and mathematics than having a robust conceptual ground in social sciences. The terminological evolution gives a glimpse of how the understanding of the idea of algorithm changes with(in) publics. Thus, the idea of an algorithm requires deliberation of its own.

The term *algorithm* has no uniform definition, so to begin with most conventional understanding about algorithms, R. Kowalski describes algorithms in the very specific sense of computer implementation as the summation of logic and control, where logic represents the understanding of a problem and control is about the strategies to solve that problem. The history of algorithms is embedded within the history of logic, i.e., instruction-based procedures for solving mathematical problems, but these are now applied to other areas of life. Algorithms are also referred to as the components of software that form the information and communication infrastructures. For such a conclusion, P. E. Ceruzzi [Ceruzzi P.E.,1998: 80) consider algorithms as "the set of instructions that direct a computer to do a specific task." Further, when algorithms are also denoted as instructions, A. Goffey [Goffey A., 2008: 17] states that algorithms "do things and

their syntax embodies a command structure to enable this to happen." The formality and technical undertone in these definitions impede the understanding of algorithms in different publics, and the sense of an informed understanding of the algorithm is lost. Although, the government and industry are trying to create standards for various algorithmic actions which have to be based on the uniformed definition. Lum and Chowdhury argue for this same reason that the description of an algorithm should be based on their impact [Lum R., Chowdshury K., 2021]. They argue that by focusing on the output, avoiding the technical complexities of the input aspect of the algorithm. This argument offers us the opportunity to focus on the themes that affect us, regardless of whether it is an algebraic formula or artificial intelligence. This line of argument has allowed us to dive deeper and scrutinise the idea of an algorithm with respect to the culture they exhibit.

Although in 2019, Algorithmic Accountability Act (HR2231) was introduced in the U.S, which tried to standardise the meaning of algorithm using the term "automated decision-making system" and defining it as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers" (Text — H.R.2231 — 116th Congress (2019–2020): Algorithmic Accountability Act of 2019, 2019). It is imperative that laws and legal rules would come up for algorithms on various accounts in the future. So, for the precedential nature of law and holistic policy-making, understanding the term and how the public associate with it is essential. Though HR2231 includes a broad definition of the algorithm, it avoids major perplexities like the distinction between high and low-risk automated decision making, the non-linear nature of software development, and only considering large technological companies.

2. Multiplicity in Meaning

Societies in the wake of the pandemic have swiftly digitalised platforms for most of the human activity. People are experiencing algorithms such as ranking, profiling, tracking, recommending, filtering. The algorithms work through both human subjects and objects shaping behaviour, way of thinking, preferences, and tendencies. These algorithm functions are made possible by their features like autonomy, decision-making power, and value-laden nature. Thus, algorithms have logic and control and help in subjective and more complex notions, i.e are able to decide what is essential and what is not [Tufekci Z. et al., 2015]. Striphas describes these phenomena with regards to digital processes as *Algorithmic Culture* [Striphas T., 2015].

Pierre Lévy, the French sociologist and philosopher, is one of the most important thinkers in the field of virtual culture. His enthusiasm focuses on the cognitive and anthropological dimensions of the Internet. Lévy defined cyberculture as a set of substance and intellectual theories like practices, attitudes, and values that emerged along with cyberspace. He defends this idea by arguing that cyberspace was a product of real social movement, as the personal computer was created by people who wanted to develop new information bases to revolutionise societies [Levy P., 2001]. Thus, along with the personal computers came digital networks, which coincided with aspirations of cultural streams and echoed with the development in communications and intelligence. Lévy has highlighted four functions: production of data through software or audio-visual devices; cleaning of data, sounds, and images; transmission by using digital networks; storage of data [Teixeira A.S. et al., 2017]. The functions are even valid for the current digital platforms. According to him the digital models are not to be read but to be interacted with, as the knowledge in this system is produced by simulation. The manipulation of parameters and simulation of all circumstances by the software gives the user a feel of a cause-and-effect relationship. Lévy's characterisation of cyberculture can be seen true as the society is facing new complexities caused by change in thinking provoked by intellectual capacities of cyberspace. The question that arises from his work is that are we structured enough to face the complexities of cyberspace. Further, his arguments lead us to the debate of technological determinism and the social dimension of technology which are part of the science and technology studies.

Tarleton Gillespie [Gillespie T., 2016] brings an exciting perspective to the algorithm debate; he is more concerned with semantics. He implies that the word algorithm could mean different for different publics. For software engineers, algorithms are simple procedures, but they are something unattainably complex for the broader audience. With this argument, he describes algorithms as a Trick, Synecdoche, Talisman, and Committed to Procedure.

Gillespie elaborates that algorithm is merely the procedure that addresses a task as operationalized for algorithm to be a trick. Additionally, to improve an algorithm is rarely about redesigning it rather it is about tuning the parameters and limits. To explain algorithms as synecdoche, Gillespie borrows from Goffey that algorithms' actions are part of an ill-defined network. It is this ill-defined network that we refer to when using the word algorithm. Further, algorithmic systems are not standalone, they are massively networked, and users tune and tweak them; thus, we need to examine the logic which guides these people [Seaver N., 2013]. In this sense, Gillespie

says that qualifying sociotechnical assemblage an algorithm allows to avoid the need to understand different elements like models, cleaning, sorting etc.

The technology industry quite often does the invocation of the term algorithm for the wide public. Calling a process or service an algorithm is associating it with the idea of being logical, mathematical, independent. That is making it the pinnacle of objectivity. Thus, the results provided by algorithms wear complete legitimacy, so the notion of algorithm acts as a talisman.

Subsequently, as Gillespie claims, the word "algorithm" is lately being used as an adjective rather than as a noun. The terms like "algorithmic identity", "algorithmic regulation", "algorithmic power", "algorithmic ideology", or "algorithmic culture" highlights this social phenomenon. These ideas include algorithms and the networks in which they function, the people designing them, data, and users. Through this, he deduces the invocation of the term algorithmic is not an algorithm per se. Still, it is about the insertion of the procedure in the knowledge system and mainly social experience. Further, Gillespie points out that, "we rarely get to watch algorithms work; but picture watching complex traffic patterns from a high vantage point: this algorithmic system privileges the imposition of procedure, and— to even participate in such a complex social interaction— users must in many ways accept it as a kind of provisional tyranny."

These notions about algorithms make it clear that there is sense of friction between human sociality and procedural systemisation. But algorithms are at the centre of the network technologies we are surrounded by, and human life is increasingly dependent on them.

Through historical analysis, Ted Striphas has tried to trace the conceptual understanding of the emergence of algorithmic culture by focusing on the words that substantially affected the culture. He claims that the cultural work has been passed on to the digital technologies using computers and databases, which has rearranged some of the words closely associated with culture. Striphas, like Gillespie , focuses on the semantic dimensions of algorithmic culture, and both derive their inspiration from Raymond Williams' book "Keywords" (1983). According to Williams, the term "culture" previously has been a relatively vague word, but since the beginning of the 20th century it has become one of the most complicated and multifaceted notions. To conceptualise this understanding he traced semantic shifts among certain terms which formed the basis for his book.

Striphas , for his case, identified three words: "Information", "Crowd', and "Algorithm". Using etymological analysis, he has tried to map the threshold of the meaning of these selected words. However, he sketches the

history of the word information from the 12th century to modern times. To summarise his effort, cultural life is becoming a type of information processing task among many other affairs. Further, he believes "humans no longer hold exclusive rights as cultural producers, curators, or interpreters, which has been passed to the digital technologies" [Striphas T., 2015]. This brings the question of uniformity between humans and technologies as to what would happen if the cultural practices and decision-making arguments were not well-informed.

Similarly, for the word "*crowd*", Striphas founds parallels with *community* or common culture, as proposed by Williams, the word relates to the denial of individuality or full participation, and this has its shadow over the words like *crowdsourcing*, *collective intelligence*. Williams affirms that solidarity is an essential element for the sustenance of common culture, but what he could not predict was the computational nature of solidarity that exists today.

Striphas identified that the word *algorithm* comes from the word *augrim* or its more conventional version *algorism* following orthographic transformations. But he emphasises that the semantic perspective of the word *algorism* includes secondary meaning that is key to the manifestation of the algorithmic culture. He further moves on to the papers by Ralph Hartley and Claude Elwood Shannon, both of whom worked at Bell Laboratories in the United States. Hartley was more focused on the process of communication, but Shannon was more concentrated on the signal and noise as he believed communication is something to be engineered rather than letting uncertainty seep in. Consequently, Shannon believed in devising an arrangement of procedures or algorithms that could cascade with the governing process of communications. This, Striphas believes, is among the first algorithmic theories of information.

Paul Dourish initiates the discussion on digital culture by contemplating the work of Niklaus Wirth [Wirth N., 1975], who advocated a structured approach to programming in the area of design and software engineering. Wirth's approach was to dissect problems into smaller bits and then follow a structured approach to solve them. Such an approach helped in the easy development of computer programs and their analysis. Wirth also focused on the importance of the relationship between data structures and algorithms. Skipping the technical differences between program and algorithm, Dourish concludes that it is essential for us to understand algorithms in connection with computational procedures such as data structures. Dourish further concludes that "the limits of the term algorithm are determined by social engagements rather than by technological or material constraints." He argues

that the boundaries of the term algorithm are the social boundaries, i.e., between technical people and non-technical people, who may not understand the explanations in play. This conceptualisation of algorithms by Dourish uses a different approach from the previous inquires on algorithms carried out by Striphas (2015) and Gillespie (2014, 2016).

Nick Seaver's [Seaver N., 2017] approach to algorithms is in response to the most usual definition of the term *algorithm* in computer science. Seaver builds on the work of [Devendorf L., Goodman E., 2015], who opted for a new approach towards algorithms by arguing that algorithms are multiple systems otherwise assumed as singular and material accumulations rather than protracted texts which opened new entry points for critical practices in design and engineering. Another interesting inclusion in the study by Seaver was developed in the works of Annemarie Mol [Mol A., 2002].

Mol's work is an ethnographic study of atherosclerosis; instead of restricting the topic to theoretical definitions, she investigated how atherosclerosis problem is being understood in practice in a Dutch hospital. Her STS analysis is a rich multi-layered text with an undertone of anthropology but also with contemplation on the multiplicity of reality in practice [Jensen T.E., 2005]. Thus culture, in reference to Mol's work, as Seaver writes, is "not one coherent thing, nor is it a set of disparate things, such that every person enacts and imagines their own in isolation."

Seaver also elaborates on the terminological anxiety of word "algorithm"; for him, a terminological definition is about drawing the boundaries for the disciplinary authority of critical algorithm studies. But rather than offering the concrete definition, Seaver tries to look into an anthropological approach because anthropology for him is a valuable tool for thinking through the engagements between incongruent knowledge traditions. The ethnographic approach to algorithms essentially helps critical scholars in understating the formalist approach to the culture.

While deliberating about algorithms in culture, Seaver elaborates on the work of Dourish, where he hinges his arguments on the definition as a set boundary. Seaver argues from the merit of his ethnographical work that the term algorithm's meaning evolved even between two technical people. What he finds interesting is that scholars could say for an emic definition of the word algorithm, but we cannot know these definitions in advance. He also points out that technical people are not the only crowd responsible for generating the algorithms; thus, a very diverse group of people with varied skillsets produce algorithms. Seaver essentially feels that a more precise definition is mainly used to isolate the concerns of algorithms from the

social sciences or critics of algorithms. His understanding of a proponent of facial recognition and a critic of recommender system is situated in the fact that both rely on the deductive distinction between culture and technical people. This is what he refers as the *algorithm in culture* i.e., the notion about algorithms centres around the belief that they are discrete objects and could be located in the cultural context. Algorithms themselves are not culture, they could shape culture or might be shaped by it, but they are two different things.

The scepticism in term "culture" as a concept of study has been a common place among anthropologists. The problem began from homogenising the political nature of essential tendencies of culture, and the speed of life changing [Abu-Lughod L., 1991]. The concept of culture has evolved from the traditional domain and has found its dominance in ethno-nationalism, business establishments, etc. While a social scientist could criticise the people's use of culture, these users are usually the influential part of the culture. Bourdieu takes the practice approach towards culture, where he points out that many anthropologists view culture as an order of practice as part to form a cultural life [Burris B., 1980]. But rather than the setting of practice, culture might be something people perform. Thus, Seaver is more interested in the multiples of culture, i.e., culture not as a unified means instead of loosely collaborative practices that sometimes compete or interact. He takes supports Mol's ethnographic work and case studies by Laura Devendorf and Elizabeth Goodman for this conclusion. To understand this as an argument for algorithms, different actors shape algorithms in different ways, technical people try to mediate by coding, and some non-technical people see it as magic. But, as Seaver writes, "no inner truth of the algorithm determined these interactions, and non-technical outsiders changed the algorithm's function: machine learning systems changed in response to user activity, and engineers accommodated user proclivities in their code" [Seaver N., 2017].

The above-discussed literature on the conceptualisation of algorithms in culture and culture in algorithms presents an opportunity to explore the concept of the term *algorithm* within society and how society shapes the notions on algorithms. The significant gap that exists is the lack of empiricism in the methodology to understand the algorithmic culture.

3. Ideating Algorithm through Concerns

With no set boundaries pertaining to the definitional clarity on the term *algorithm*, algorithmic concerns help define the scope of the algorithm. But, as the advancements in information technology are seeping into our

lives more than ever, we can now create more customised services and outsource specific routine tasks such as shopping, vacuuming floors, education, etc. Still, everything has a potential cost attached to it. In a larger context, concerns over jobs, ways of social interactions, virtual reality, etc., had been discussed, though algorithmic concerns are the result of the application of algorithms. But algorithmic concerns evolve in due process of the application. So, to ask, are we designing algorithms, or are algorithms designing us?

The heterogeneity in algorithmic concerns raises the argument about the understanding of algorithms; thus, the more we inquire, the more accurately we can understand their essence. Therefore, without deep-diving into the literature on each concern, the strategy is to focus on the case studies to understand how law and policy-making build its perception around the term *algorithm* through various cases.

M. Kranzberg (1986) writes: "Technology is neither good nor evil; nor is it neutral" as his first law of technology. Even though algorithms to the general publics are "mysterious and inscrutable machinations of big data, big government, and big business increasingly part of the infrastructure of the modern world, but hardly a source of practical wisdom or guidance for human affairs" [Christian B., Griffiths T., 2016] or is becoming a guiding force. Still, people fail to recognise or are ignorant of its effect. In the current phase, algorithms interact with humans in the form of technology, and the fact that it has become a part of our life makes it scrutable. To scrutiny is to raise the concern over the black-box nature of algorithms. Another point that raises concerns is when making an informed decision, the very act of informing jeopardises the outcome.

Against the claims of what algorithms can do, they deserve some scrutiny, but it is essential to know what to scrutinise before that. We have tried to highlight specific concerns about algorithms.

A. Bias

One of the standard and important concerns about algorithms is bias. The explosion in the widespread use of algorithms has introduced biases created by algorithms at the forefront of technology, academia, and media. Even policy-neutral algorithms had, in some cases, imitated historical inequalities and societal prejudices [Tene O., 2017]. *Bias* as a word that primarily implies a negative connotation, i.e., it has to be avoided or is problematic. Instead, in this article, we would take a more neutral approach for the term *bias*; as Danks and London explain, the term is about deviating

from a standard. To elaborate, a moral bias would conclude to a deviation from a moral norm or, in any case, social bias, regulatory bias, etc. To synthesis, the point is that something can be biased based on one view but not by another view. Although bias can exist in various forms, which can also be subdivided, not all forms are on par with each other. A section of academia believes that these value-laden arguments cannot be solved just by technology [Danks D., London A., 2017]. Some might be more problematic, and others might be a result of an ethically desired system. There are numerous examples of algorithmic bias, but some have caught the headlines like the racially bias algorithm in Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) used in the United States to provide sentencing advice, Google's advertising algorithm, which appeared to be gender-biased by showing higher-paying jobs to men than women, etc. [Koene A., 2017].

It is important to deliberate on the case of the COMPAS algorithm to understand why there is a need to scrutinise the algorithm and how is the system is biased. This is about the epistemic agency[3], as [Rubel A. et al., 2018] write. To have a convincing level of agency, a person needs to know where they stand even though they might or might not have the power to take action. The basis for this argument is that people are reasonable beings who are also part of a community. So, people and institutions related to us exercise power over us, matter for us. Thus, denying someone the ability to understand the reason for the action taken against them is a failure to respect them as an agent. In a similar context, one can find superficial information about the algorithm used in COMPAS, but getting access to the algorithm is impossible. This implies people lack access, and without access, they cannot improve their understanding of how they are being treated by COMPAS. But the argument is two-fold; that is, in the case of both the COMPAS and the judge, the root cause of the problem is the inscrutable process. For COMPAS, it is the algorithm, and in the case of a judge, it is his mindset. The argument begins with the effect of the agency. Judge psychology could be as obscure as the algorithm of COMPAS; thus, the purpose of understanding the reason would fail. But there is a difference between human and algorithm in making the decision. The former one is culpable, but the latter cannot be made morally responsible. That being said, as Rubel et al. concurred algorithms are not agents.

To sum up the argument, if the algorithm of COMPAS gets it wrong, the moral responsibility lies with the person or the group responsible for

[3] Epistemic Agency can be explained as learning efforts taken by oneself and the advancement in understanding.

developing and designing that algorithm. It is important to consider European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, stating "a data subject has the right to an explanation of the decision reached after (algorithmic) assessment." However, the extent of the right to an explanation depends on the court, and its interpretation is yet to be seen [Voigt P., von dem Bussche A., 2017].

The biases in algorithms seep into our lives through its most common implementation, i.e., computer systems and the internet. There have been numerous accounts where the software or the internet has shown to contain biases that both unjustly and systematically discriminate or favour certain individuals or groups. As [Bozdag E., (2013] points out about the current trend of personalised algorithms, though it had existed since the 1990s but are now part of a much-blown idea of algorithmic filtering due to the availability of cheap and efficient infrastructure and also due to the increased popularity of social networks and search engines. To increase relevancy, it utilises interpersonal information about the users and tailors that information according to the need. This is where the biases percolate and have severe implications on human values, transparency, trust, privacy, etc. [Granka L.A., 2010] also points that information diversity is a relevant function of bias, which implies, for example, if a social media platform exercises a bias with respect to an advertiser, then it would be limiting the diversity and democracy integral to information. Even the IEEE project on Algorithmic Bias Consideration is primarily about providing a clear picture to the organisations dealing with algorithms on how algorithms are assessing, targeting, and influencing users.

B. Privacy

Amongst all the development in information and communication technology an extremely prominent issue is privacy. With the ever-increasing use of social media, search engines, and the power of algorithms to influence people's choices, people themselves grant their privacy with their own hands to the government or the private organisations, and then things like the Cambridge Analytica scandal wakes them up. These recent examples, have made clear the crucial importance of privacy. This brings another question, that who can make the decision about the privacy of others, and how these decisions can be made [Goldberg L. et al., 2001].

Privacy, as in law and ethics, is a blanket term and, in a loose sense, means "having control over the information about oneself" [DeCew J.W., 1986]. It is critical to this analysis that we discuss the concept of privacy in a

more elaborative sense to make the argument more visible and exhaustive. To begin with the definition of privacy, [Parent W.A., 1983] defines privacy as "the condition of not having undocumented personal information (knowledge) about oneself known (possessed) by others." The definition by Parent is motivated by the fact that it should be easy to understand and should not cross over to the boundary of other related concepts. He goes on to defend the point that his definition is more about the moral value of protection of someone's freedom and individuality against a gratuitous invasion.

Additionally, it is essential to understand what information is considered personal. Firstly, it includes facts that people do not want or choose to reveal to society (except family and friends) or information about which an individual is sensitive even though similar information about other people may be widely known . Parent not only sees privacy as a coherent concept but also believes there is a degree of uniqueness and fundamental value attached to it. In contrast to Parent's view about privacy, [Thomson J.J., 1975] argues that the right to privacy is derived from other rights, mainly property rights. Her approach is considered reductionist, as according to her, there is no such thing as the right to privacy, and for any violation of the right to privacy some other non-identical right is violated. What strengthens the Parent's claim is the reverse reductionism of Judith's idea about the right to privacy [Fried C., 1984] broadened the previous approach and defined privacy as not only the absence of information about us in the mind of others, but it is about the control of information about us. The idea of privacy is also based on trust, i.e., other people would display integrity, reliability, justice, and other ethical behaviour.

Further, the European Union's General Data Protection Regulation (GDPR) has connected the right to privacy with human dignity. As Article 88 of GDPR points out, rules would include appropriate and explicit measures to protect the data subject's *human dignity* by taking into account the due process and transparency. However, human dignity does not come up in GDPR but is fundamental to its core and is an important consideration when interpreting privacy ('European Parliament and Council of European Union (2016) Regulation (E.U.) 2016/679,' 2016). [Floridi L., 2016] elaborates that in post-modern philosophy, lack of privacy could arise due to the fact that mutual recognition encourages it. Thus, explaining the circumstance of why we care so less about what we share online. Floridi goes further to make a point that the philosophy of information assumes human nature in the form of an informational pattern and argues that under this consideration, a breach in privacy has an ontological influence.

In the digital world, the algorithms employed by search engines and platforms track and cater to individual behaviour to provide recommendations. Still, this data is not necessarily created by them solely but still end up on internet as a result of public, government, and other databases. This makes internet footprints of the individual without any online accounts. In that sense, an important idea which European Union's GDPR has embraced under Art. 17(2) make the concept of privacy more robust with the concept of the Right to be Forgotten[4]. The inception of this right can be traced back to the judgment of the Court of Justice of the European Union, where the court ordered Google to remove debt recovery details of a Spanish citizen (Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014). Following the precedence set by the Google ruling, countries like France have both civil and criminal counts on privacy.

In context of India, the judgment by the Supreme Court of India in Justice K. S. Puttaswamy (Retd.) and Anr. Vs. Union of India and Ors., which was about the constitutional validity of Aadhaar an Indian biometric scheme, was instrumental in shaping the notion of privacy in India. The judgment endorsed the right to privacy as a fundamental right; the one-page order read, "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution" (Panday, 2017). The judgment acknowledged that privacy is an aspect of human dignity and also advocated for the creation of a legal framework around the privacy concern (Puttaswamy v. India, 2017). With the above conception of privacy in the Indian context, the right to be forgotten has found its place in Personal Data Protection Bill, 2019, which had been missing from the Information Technology Act 2000. But the balancing test it faces is yet to be seen.

There is a belief that when algorithms compute *correct possibilities,* they are exempted from being considered harmful to privacy and many other things since they produce exact output for the given input. But, when it comes to subjective decision making, which does not have a correct answer, this may involve relying on algorithmic operations applying a large number of metrics and different things. Tufekci believes this is where the argument about privacy begins. An example of this is how the popular mobile game *Pokémon Go* required access for the entire *Google* account on *iOS*, including emails, browsing history. Similarly, *Uber,* in one of its updates, collected

[4] The right to be forgotten gives the right to the individuals to correct, restrict, delink or delete their personal information on the internet platform.

user location even when people were not using the application on their mobile [Hayes D. et al., 2017].

It is important to separate the idea of violation of privacy through algorithms and social media through an interconnected area, as algorithmic concern is a far more significant problem than privacy invasion.

Today, every website people visit and every software they use flashes, "your privacy is important to us." Still, users evaluate this on varying factors like the investment in privacy, type of information collected, and its use, but recent cases have displayed the above pretence being not so robust. Some scholars consider that with technology evolving, the loss of privacy is inevitable. PEW Research published a report Digital Life in 2025 in 2014, which revealed that "everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great that continuous monitoring will be the norm" [Anderson J., Rainie L., 2014].

C. Design

With the increase in the scope of algorithms, the future application of algorithms is becoming ambiguous. This makes it more difficult to predict the future use, thus posing the question that was the design ethical enough to cope with the future scope? Every technology which finds its way to society will arbitrate human experience, action and, in the end, helps in forming moral decisions [Verbeek P.P., 2008]. [Freidman B., Kahn H. (2002] put a very interesting argument in the sense of design and ethics. Their reasoning is based on the view that in computer science and technology literature, the word *trust* is frequently used as synonymous with *security*, even though these two terms mean different in ethics. They go further by detailing out that there two ways of design can help in making online interaction safe. One way is to move towards solutions like passwords, encryption, locks, etc. The other idea is to understand how a trust-based relationship can be fostered and created, therefore designing systems around them.

There is a point of view that technology influences humanity also by the function of its design, in the context it is used, and the people are involved. The process of design, implementation, and adoption of technologies is complex, and within it, algorithmic concerns have very little influence on the designing process. A significant portion of the ethical design in algorithms is related to dataset, as biases in the dataset can be mitigated to the designing process [Brauneis R., 2017]. This can be elaborated with an

example of biases in Amazon.com Inc's recruiting engine, which was later shut down. Since 2014 Amazon was utilising an artificial intelligence tool to sort resumes [Kearns M., Roth A., 2020]. But in 2015, they realised the system was not gender-neutral. It rated male resumes higher than female, even though Amazon edited the program in particular terms to make it more gender-neutral but the system taught itself to find ways to search gender by using terms such as all women college, women's club, etc.; finally, the program was abandoned. The cause of this problem was the model, which was used to train the program, that consisted of previous ten-year resumes which were mostly of men; thus, the machine realises that women are not preferred. The root cause, in this case, was not some apparent negligence on the part of the development team. The resulting algorithmic bias was the unanticipated outcome of abiding by the standard procedure of machine learning. Thus, beginning from the specified objectives mostly for efficiency or accuracy or both and algorithmically exploring the model that maximised it by using a large amount of data. In turn, revealing the design flaw of the solution proposed by the designer.

The idea of design ethics also goes beyond just the inherent value of the work itself; it should also align with the values of designers and industry. In this networked society, data-driven designing of algorithms is proposed for good but often has ulterior motives. There are ways to address these issues by utilising frameworks such as *human in the loop*[5] and *society in the loop*[6]. Conversely, we lack the comprehensive practicality to transform values, organisational, and societal realities into the process of algorithm designing. [Martin K., 2019] believes that algorithms are embedded with morally important decisions taken by firms and individuals, which have specific implications on accountability, and design decisions can amplify the role of algorithms. Abelson and Sussman's phrase "programs must be written for people to read, and only incidentally for machines to execute" captures the essence of design in algorithms.

Recently, as our understanding of technological innovation, competitiveness, or in the case of creativity have increased, there is a growing sense that a design-thinking perspective must be induced in it. On a similar notion, we have privacy by design. Privacy must be incorporated into organisation values, objectives, design processes, and planning rather than introducing it at the end of the process. [Campisi P., 2013: 364] defines the

[5] Human have monitoring and supervisory control at the important junctions in the system.

[6] Society in the loop in short is human in the loop in addition with social contract.

principle of privacy by design as "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use, and ultimate disposal." Privacy by design is more about preventing breaches from occurring than just providing a solution for settling them. According to Article 25 in GDPR, companies involved in processing personal data should device fitting measures and defences which observe the privacy principle and such should be built into the system by default (European Parliament and Council of European Union (2016) Regulation (E.U.) 2016/679, 2016). Even though GDPR has a detailed description of privacy by design, it is still not clear about the obligation to ensure it and the technical specification part. As Christl, Kopp, and Riechert wrote: "Systems that make decisions about people based on their data produce substantial adverse effects that can massively limit their choices, opportunities, and life chances."

D. Transparency

A common phrase for reference to algorithms is black-box, used to define its opaque nature. Transparency acts as a tool for ethical development and tries to make use of algorithms in such a manner that they promote human rights and aid society (European Parliamentary Research Service, 2019). The opacity around algorithms can be highly complex due to the involvement of machine learning, which is not only dependent on design choices but also on the data it is trained. The value proposition of transparency is not about being a tool but about the purpose it serves. Looking at the recent attention on transparency as a mode of algorithmic accountability, it is important to consider what transparency brings to the table or how it has functioned historically and technically.

To begin the discussion about transparency, firstly, we need to understand the idea of opacity in algorithmic applications. As [Burrell J., 2016] writes, opacity can be of various forms, beginning with the secret kept by state or corporate as a strategy of self-protection or coping with the competition. Search engine optimisation is a classic example where big corporations do not reveal their algorithms for ranking, filtering, and recommending searches. But the open-source movement has tried to change this notion. [Diakopoulos N., 2015] believes that making code available for review under certain regulations can also be a way forward. Secondly, opacity also occurs since coding and designing algorithms is a specialised skill both in terms of reading and writing, which makes it unapproachable for the ordinary population. As [Mateas M., Montfort N., 2005] have concluded,

codes that are written in a holistic manner perform *double-duty*, that is, to say that it can be interpreted by the programmer and someone maintaining the code and as well as by the machine utilising it. Then, within this arises issues like diversity and mass dissemination of the algorithm for common use. Lastly, Burrell argues about the scale of scrutiny of algorithms which poses an opacity dilemma even when we decide to audit these algorithms. The argument is not per se about the inability to scrutinise but about the point that specific algorithms, for example, in machine learning, are so extensive, interlinked and require large datasets to test. Even then, every dataset cannot be tested, thus being opaque.

After an inquiry about the opacity in algorithmic operations, it is important to understand the aim of transparency or, in that case, what transparency is and why do we need it, and from whom. Turilli , Floridi (2009) argue that transparency is not inherently an ethical condition, but it enables the conditions fostering it. Secondly, they point out that transparency has at least two different connotations, which are usually used similarly but are deceptive. For business ethics, information ethics, and information management, transparency is about the visibility of information, which can be increased by removing obstacles. However, in the case of disciplines like computer science, transparency is about information invisibility.

Historically summarising, transparency is not a result where everything is clear and evident, but it creates a system of perceiving and knowing that maintains a form of control [Phillips J.W., 2011]. The idea of transparency leads us to be accountable, but if transparency has no meaningful effect, it can lose its purpose. The meaning of transparency also depends on the use and type of algorithmic operations, i.e., which aspect of algorithms like codes, logic, goals, variables, etc. Thus, algorithmic transparency is about seeking insight into the system's behaviour about any input, trying to get an explanation for the output.

Accountability is a consequence of transparency; hence, we cannot hold anyone accountable if we do not know what and where things are wrong. So, it is important to understand the areas where transparency is demanded. Transparency in the algorithmic system can range from transparency in data, goal, outcomes, influence, compliance and usage (European Parliamentary Research Service, 2019). In the argument about transparency, it is essential to understand who gets to view what. The potential viewer might be everyone, certain parts made available for the public, researchers, accreditation agencies, third-party experts, etc.

To concretise our arguments about transparency, it is important to put it in with relevant cases. Many financial services use all sorts of algorithms to process loans that are not transparent in their function, as people might know the reason behind their loan rejection. Another example is the Yelp review filtering algorithm, which created dissatisfaction among users for being opaque and manipulating businesses to pay for advertising in return for the higher rating. Yelp not only hides the way its review filter works but even hides its existence altogether [Eslami M. et al., 2019]. Even the idea of transparency is not infallible, merely seeing what is inside the system does not provide any understanding of its comportment [Ananny M., Crawford K., 2018].

E. Liability

The majority of our interaction with the algorithm takes a form of product or services, but as the birth of commercialisation of products could be attributed to technological advancements and globalisation of human efforts, this has also created a problem of lack of liability, which is more than true for algorithmic systems. There are numerous examples in which it would be difficult to attribute liability, like in the case of Samathur Li Kin-Kan, who filed a suit against the salesman who convinced him to put a large piece of his wealth for stock trading with the help of a supercomputer (K1) [Elish M.C., 2016]. Today, most software, website, program, etc., are built from preconstructed algorithms, which act as a base for them. It is also essential to differentiate between the term's accountability and liability as both are used as synonyms most of the time. Nissenbaum (1996) wrote that difference between accountability and liability is mainly a legal one. Liability is *evaluated* on the victim's plight, whereas accountability is about the relationship of the agent to the outcome. To sum this, liability tends to bind more largely than accountability. It is more about the actor than the action, though their efforts might contain the liability [Haines N., 1955].

Giving algorithmic subjects the right to understand the logic behind the cryptic system is seen as the first step towards an intelligible society [Hildebrandt M., 2014]; [Pasquale F., 2013]. Even GDPR includes clauses for an individual's right to demand a description for *logic* behind the automated operations made for them, thus enabling the public to examine and challenge these opaque systems.

Liability for the system can include hardware and software. Though hardware liability would be easy to define, the software liability is difficult to put on. The producer of the algorithm could theoretically be held

responsible for the defects, but this rarely occurs in practice [Tjong Tjin Tai E., 2018a]. The contractual liability is limited by the disclaimer of warranties, and product liability ceases to exist due to the intangible nature of the software (algorithms). M.C. Elish argues that the discrepancies between liability and control when control is shared by many actors (human and algorithms) and its implications for legal regulations and liability. She developed the term moral crumple zone to identify the ambiguous nature of "distributed control, automated and autonomous systems[7]". It is similar to the crumple zone in a car, designed for the purpose of absorbing the force of the crash; similarly, the human takes all the wrath of the moral and legal obligations when a system ill performs. This emphasises the structural feature of the system, which might take undue advantage of human operators. Liability is more part of a governance issue in algorithmic decision making, but this research would not try to explore the governance field.

When viewing the liability aspect, it is imperative to scrutinise the legal personality of algorithms: anything or anyone the law recognises as a legal actor is considered a legal entity. Thus, legal entities can enter in a contract, can be sued, and can sue. [LoPucki L., 2018] suggests that an entity can be recognised as algorithmic if it is controlled by an algorithm. The creators of algorithms have not discarded the idea of them being a controller with the condition that users do not modify the algorithms in use. Although the algorithm has no rights of its own, Bayern et al. (2016) point out that by preparing algorithms as a legal entity, it can be given the power to exert the rights of an entity. Thus, the concerting idea of the personhood of the algorithms. But presently, algorithms are not recognised under any legal entity. The algorithm as the software is protected under the Copyright Act, 1957, in India [Nayak S., 2013].

Data and algorithms are inherently connected to each other. Thus, data need algorithms to be meaningful, and algorithms without data are just a dead horse in this knowledge-based society. With an understanding of how this combination affects society at large, the need for liability arises. Algorithms, in some instances, require databases either to train or to develop the algorithms for them to function. These databases, in India, are protected under Information Technology Act, 2000; Indian Penal Code, 1860 and supplemented by Copyright Act, 1957 and Indian Contract Act, 1872 to tighten further the grip on data mishandling [Shabana N., 2015]. However, these laws per se do not consider the liability of any mishappening resulting from the algorithms themselves.

[7] Related to computational technologies.

The increasing autonomy of the algorithmic systems also acts as an impediment to holding humans liable, but this autonomy is a function of scale [Karnow C.E.A., 1996]. Certain systems work only on their own for small tasks like trading algorithms, which also requires permission when boundaries are reached. In contrast, a computer virus runs without any possible intervention or communication from its makers at times. Even though autonomy is a relative concept and can be interrupted by an outside force, with such references to autonomy [Bertolini A., 2013]; [Beard J. , 2014] has argued that human judgment may be required for such systems and the matter of law, such systems should always be under human control. This leads us to the arena of who should be liable and under what grounds. It is crucial to determine what gives rise to the liability, that is to say, under what circumstances someone or something become liable for their action. The possibilities can range from taking inadequate deterrents while creating or designing the algorithmic system, i.e., dropping the risks on the users, which could have been averted.

Further, this also includes paying insufficient attention when owning or using a system like not floating updates for the system. Lastly, there can also be a risk-based liability, i.e., there is a possibility that any autonomous algorithmic system can produce a detrimental outcome. The only way to avoid such an outcome is not to make such systems, which is not an option [Tjong Tjin Tai E., 2018b].

Under the circumstances such as the above provides the ground for liability, thus it important to investigate the fact that who liable. In most specific cases, liability rests on the person in a spot to avert the harm; to rephrase, the person in control of the environment or system. Many a time, various people occupy such positions, but certain positions stand out in terms of liability, as Tjong Tjin Tai mentions, firstly, the producer of the algorithmic systems. The producer can be the designer or creator of the system, thus reducing the risk. Secondly, the owner of such systems has the control to alter and restrict the system. More than often, the owner is deemed liable as it is easy to identify the owner. Lastly, the operator of the system, as this is the position that has the power to control and direct the system, thus can prevent the damage. The position of liability cannot be restricted to these positions as the algorithmic systems are increasing their exposure.

To understand the complexity of liability, let's take the case of the Tesla autopilot car crash. In March 2018, an Apple employee died after his Tesla car crashed into a concrete barrier in Silicon Valley [Rushe D., 2020]. The

US. National Transportation Safety Board (NTSB) investigation found that the car was in autopilot mode (semi-autonomous) using Tesla Autopilot algorithms. The driver was found liable since he was playing a video game while driving in semi-autonomous mode. Even though Tesla instructs drivers to keep hands on the driving wheel while in autopilot mode. But the NTSB report further implied that the Tesla autopilot system did not provide the "effective means of monitoring the driver's engagement." NTSB chairman said, "If you own a car with partial automation, you do not own a self-driving car. So, don't pretend that you do" (NTSB, n.d.). The critics also pointed out that Autopilot branding gives drivers an illusion that cars can drive themselves fully autonomously. It is visible that liability is not easy to exercise when power dynamics come into play. Still, as the case is in court (Siddiqui, 2019), its ruling will help us to improve our rationale on liability.

Conclusion

From being attributed to culture or evolving inside the culture, the algorithm had become equally contested as the word *culture* itself in terms of the terminological anxiety they both raise. The boundaries of the definition of "algorithm" are vague. So, it is important to understand that the multiplicity in its meanings and offers us more proof of its effects and how it has become part of sociality. The more we probe the term *algorithm* with respect to different academic streams, the multiplicity increases, which results in refining the understanding as the meaning evolved for various public to even becoming multiple with the same set of publics.

Concerns arising from algorithms also add substance to the different meanings attached to it. The difference in experience with diverse sociotechnical assemblages utilising algorithms yields a different set of problems though not for everyone; still, the scope should exist to acknowledge those future complexities. Thus, ethnographic and anthropological studies are required to expand and interpret such experiences.

A significant point of consideration is the fact that technical people are not the only ones engaging with and producing algorithms. A diverse set of people with varied skills, when interacting with algorithms, produces an additional set of networks involving them. Thus, simplicity in understanding algorithm offered by computer science is deceiving in regard to dependency attached to it in the networked society. Their definition closes more doors of exploration by shutting the larger publics out of its scope. Thus, it is imperative for social sciences to explore what affects the society. Standardising the definition of algorithm although helps in the law and

policy making process but also restricts the stakeholding in terms of how and whom it affects.

Even though different nations and groups are coming with various legal approaches regarding automated decision-making systems or algorithms building on their standardise definitions. Though late enough, the idea of regulating algorithmic assemblages is appropriate, but without constant evolution around, the understanding would not be adequate enough to uphold the rights of the ones it affects the most.

References

1. Abu-Lughod L. (1991) Writing Against Culture. In: R. Fox (ed.) Recapturing Anthropology: Working in the Present. Philadelphia: School of American Research Press. pp. 137–162. https://philpapers.org/rec/ABUWAC

2. Ananny M., Crawford K. (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media and Society*, no. 20(3), pp. 973–989. https://doi.org/10.1177/1461444816676645

3. Anderson J., Rainie L. (2014) Digital Life in 2025. The Future of Internet. Pew Research Center (accessed: 25.11.2021)

4. Arooni J. (2017) *Algorithmic Harms: Simultaneous Results and Proponents of Privacy Violations for Individual Users*. Algorithmic Harms: Simultaneous Results and Proponents of Privacy Violations for Individual Users. (accessed: 25.11.2021)

5. Beard J. (2014) Autonomous Weapons and Human Responsibilities. *Georgetown Journal of International Law,* vol. 45, no 6, pp. 618–678.

6. Bertolini A. (2013) Robots as products: The case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, no. 2, pp. 214–247. https://doi.org/10.5235/17579961.5.2.214

7. Bozdag E. (2013) Bias in algorithmic filtering and personalisation. *Ethics and Information Technology*, no. 3, pp. 209–227. https://doi.org/10.1007/s10676-013-9321-6

8. Brauneis R., Goodman E. (2017) Algorithmic Transparency for the Smart City. *SSRN Electronic Journal*, no. 103, pp. 103–176. https://doi.org/10.2139/ssrn.3012499

9. Burrell J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, no. 1, pp. 1–12, 205395171562251. https://doi.org/10.1177/2053951715622512

10. Burris B. (1980) Book Review: Outline of a Theory of Practice. *Critical Sociology*, pp. 89–91. https://doi.org/10.1177/089692058000900410

11. Campisi P. (2013) Security and privacy in biometrics: Towards a holistic approach. In: Security and Privacy in Biometrics. L.: Springer. pp. 1–23. https://doi.org/10.1007/978-1-4471-5230-9_1

12. Ceruzzi P.E. (1998) *A history of modern computing*. Boston: MIT Press, 438 p.

13. Christian B., Griffiths T. (2016) *Algorithms to live by: the computer science of human decisions*. N.Y.: Henry Holt, 368 p.

14. Conger S., Pratt J.H., Loch K.D. (2013) Personal information privacy and emerging technologies. *Information Systems Journal*, no. 23, pp. 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

15. Danks D., London A. J. (2017) Algorithmic bias in autonomous systems. IJCAI International Joint Conference on Artificial Intelligence, pp. 4691–4697. https://doi.org/10.24963/ijcai.2017/654

16. DeCew J.W. (1986) The Scope of Privacy in Law and Ethics. *Law and Philosophy*, no. 5, pp. 145–173.

17. Devendorf L., Goodman E. (2015) The Algorithm Multiple, The Algorithm Material: Reconstructing Creative Practice. Contours of Algorithmic Life Conference. http://www.confectious.net/may-15-the-algorithm-multiple-the-algorithm-material-reconstructing-creative-practice-uc-davis/

18. Diakopoulos N. (2015) Algorithmic Accountability: Journalistic investigation of computational power structures. *Digital Journalism*, no. 3, pp. 398–415. https://doi.org/10.1080/21670811.2014.976411

19. Dourish P. (2016) Algorithms and their others: Algorithmic culture in context: *Big Data & Society*, no.11, pp. 1–16, https://doi.org/10.1177/2053951716665128

20. Elish M. C. (2016) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction (WeRobot. *SSRN Electronic Journal*, no. 1, pp. 1–26. https://doi.org/10.2139/ssrn.2757236

21. Eslami M. et al. (2019) User Attitudes towards Algorithmic Opacity and Transparency in Online Reviewing Platforms. *Human Factors in Computing Systems Proceedings*, pp. 1–14. https://doi.org/10.1145/3290605.3300724

22. Floridi L. (2016) On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology*, no. 4, pp. 307–312. https://doi.org/10.1007/s13347-016-0220-8

23. Freidman B., Kahn H. (2002) Human values, ethics, and design. In: The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications. Wash.: University of Washington, pp. 1177–1201.

24. Fried C. (1984) *Philosophical dimensions of privacy: an anthology*. Cambridge: University Press, 426 p.

26. Gillespie T. (2014) The Relevance of Algorithms. In: T. Gillespie et al. (eds.) Media Technologies: Essays on Communication, Materiality, and Society. Boston: MIT Press. pp. 167–194. https://doi.org/10.7551/MITPRESS/9780262525374.001.0001

26. Gillespie T. (2016) Algorithm. In: B. Peters (ed.) Digital Keywords: A Vocabulary of Information Society and Culture. Princeton: University Press, pp. 18–30.

27. Goffey A. (2008) Algorithms. In: M. Fuller (Ed.) *Software Studies. A Lexicon.* Boston: MIT Press, pp. 15–20. https://mitpress.mit.edu/books/software-studies

28. Goldberg I., Hill A., Shostack A. (2001). TRUST, ETHICS, AND PRIVACY. *Boston University Law Review*, no. 81, pp. 407–422.

29. Granka L.A. (2010) The politics of search: A decade retrospective. *Information Society*, no. 5, pp. 364–374. https://doi.org/10.1080/01972243.2010.511560

30. Haines N. (1955) Responsibility and Accountability. *Philosophy*, no. 30, pp. 141–163.

31. Hayes D. et al. (2017) Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application. Conference on the Information Systems Applied Research, vol. 10, no. 45, pp. 1–11.

32. Hildebrandt M. (2014) The Dawn of a Critical Transparency Right for the Profiling Era. In: *Digital Enlightenment Yearbook*, IOS Press, pp. 41–57.

33. Jensen T. E., Winthereik B. R. (2005) Book Review: The Body Multiple: Ontology in Medical Practice. *Acta Sociologica*, no. 3, pp. 266–268. https://doi.org/10.1177/000169930504800309

34. Karnow C. (1996) Liability for Distributed Artificial Intelligences. *Berkeley Technology Law Journal*, no. 11, 147 p. https://doi.org/10.15779/Z38ZD4W

35. Kearns M., Roth A. (2020) Ethical algorithm design should guide technology regulation. Available at: https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation

36. Koene A. (2017) Algorithmic Bias: Addressing Growing Concerns. *IEEE Technology and Society Magazine*, no. 2, pp. 31–32. https://doi.org/10.1109/MTS.2017.2697080

37. Kowalski R. (1979) Algorithm = logic + control. *Communications of the ACM*, no. *22*(7), pp. 424–436. https://doi.org/10.1145/359131.359136

38. Kranzberg M. (1986) Technology and History: Kranzberg's Laws; *Technology and Culture*, no. 3, p. 544. https://doi.org/10.2307/3105385

39. Lévy P. (2001) *Cyberculture*. Minneapolis: University of Minnesota Press. 280 p.

40. LoPucki, L. (2018) Algorithmic Entities. *Washington University Law Review*, no. 4, p. 887.

41. Lum K., Chowdhury R. (2021) What is an 'algorithm'? It depends whom you ask. *MIT Technology Review*. Available at: https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/

42. Martin K. (2019) Designing ethical algorithms. *MIS Quarterly Executive*, no. 2, pp. 129–142. https://doi.org/10.17705/2msqe.00012

43. Mateas M., Montfort N. (2005) *A Darkly: Obfuscation, Weird Languages, and Code Aesthetics*.

44. Mol A. (2002) *The body multiple: ontology in medical practice*. Durham: Duke University Press. 216 p.

45. Nayak S. (2013) *Copyright Protection for Computer Software an Indian Prospective — Intellectual Property — India*. Available at: https://www.mondaq.com/india/copyright/262564/copyright-protection-for-computer-software-an-indian-prospective

46. Nieborg D.B., Poell T. (2018) The platformization of cultural production: Theorising the contingent cultural commodity. New Media and Society, vol. 11, pp. 4275–4292.

47. NTSB. (2018) Collision Between a Sport Utility Vehicle Operating with Partial Driving Automation and a Crash Attenuator. Washington: NTSB, 74 p.

48. Panday, J. (2017) India's Supreme Court Upholds Right to Privacy as a Fundamental Right and it's about Time. Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

49. Parent W. A. (1983) A New Definition of Privacy for the Law. *Law and Philosophy*, no. 3, p. 305. https://doi.org/10.2307/3504563

50. Pasquale F. (2013) *The Emperor's New Codes*. P. 1–86.

51. Phillips J. W. (2011) Secrecy and Transparency: An Interview with Samuel Weber. *Theory, Culture & Society*, no. 8, pp. 158–172. https://doi.org/10.1177/0263276411428339

52. Puttaswamy v. India. Global Freedom of Expression (2017). Available at: https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hug

53. Rubel A. et al. (2018) Algorithms, bias, and the importance of agency. *CEUR Workshop Proceedings*, pp. 9–13.

54. Rushe D. (2020) Tesla driver who died in 'autopilot' crash was playing on phone, inquiry finds. The Guardian. Available at: https://www.theguardian.com/technology/2020/feb/25/tesla-driver-autopilot-crash

55. Seaver N. (2013) Knowing Algorithms. In: Digital STS Field Guide, pp. 412–422. https://doi.org/10.2307/j.ctvc77mp9.30

56. Seaver N. (2017) Algorithms as culture: Some tactics for the ethnography of algorithmic systems. *Big Data and Society*, no. 2, pp. 1–12. https://doi.org/10.1177/2053951717738104

57. Shabana N. (2015) An Indian Outline On Database Protection — Privacy — India. Available at: https://www.mondaq.com/india/data-protection/450526/an-indian-outline-on-database-protection

58. Siddiqui F. (2019). *Tesla sued by family of Apple engineer killed in Autopilot crash.* Available at: https://www.washingtonpost.com/technology/2019/05/01/tesla-sued-by-family-man-killed-autopilot-crash/

59. Striphas T. (2015) Algorithmic culture. *European Journal of Cultural Studies*, no. 4–5, pp. 395–412. https://doi.org/10.1177/1367549415577392

60. Teixeira A. C. et al. (2017) Complexities of Cyberculture in Pierre Lévy and Developments in Education. *Creative Education*, no 1, pp. 119–130. https://doi.org/10.4236/CE.2017.81010

61. Tene O. (2017) Taming the Golem: Challenges of Ethical Algorithmic Decision-Making. *North Carolina Journal of Law & Technology*, no. 19, 16 p.

62. Thomson J. J. (1975) The Right to Privacy. *Philosophy & Public Affairs*, no. 4, pp. 295–314.

63. Tjong Tjin Tai E. (2018a) Liability for (Semi)Autonomous Systems: Robots and Algorithms. *SSRN Electronic Journal*, pp. 55-82. https://doi.org/10.2139/ssrn.3161962

64. Tufekci Z. (2015) Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency. Journal on Telecommunications & High Tech Law, no. 23, pp. 203–216. https://doi.org/10.1525/sp.2007.54.1.23.

65. Tufekci Z., York J. C. et al. (2015) *The Ethics of Algorithms: from radical content to self-driving cars*. Available at: https://cihr.eu/publication-the-ethics-of-algorithms/

66. Verbeek P. P. (2008) Morality in Design, Design Ethics and the Morality. *Design*, pp. 91–103.

67. Williams R. (1983). *Keywords: A vocabulary of culture and society*. Oxford: University Press.

68. Wirth N. (1975) Algorithms Plus Data Structures Equals Programs. *Prentice Hall* (Issue August). (Prentice-Hall series in automatic computation)

Information about the authors:

Nabil Ahmad Afifi — PhD Scholar.

Reeta Sony A.L. — Assistant Professor.

The article was submitted 12.07.2021; approved after reviewing 11.10.2021; accepted for publication 01.11.2021.

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4

Research article
UDC: 349
DOI: 10.17323/2713-2749.2021.4.98.113

Legal Basis for Remote Sale of Medicines in the Russian Federation

Alexander S. Kornienko[1],
Nadezhda G. Neretina[2]

[1] National Research University Higher School of Economics
[2] Russian Presidential Academy of National Economy and Public Administration
[1] akornienko@hse.ru, https://orcid.org/ 0000-0002-0759-2921
[2] email: Nadezhdalow@mail.ru, ORCID: 0000-0003-1606-6007

Abstract

The topic of the article is very relevant, first of all, due to the fact that today the development of the information and telecommunication services market involves almost all areas of people's life in the field of e-commerce. Until April 2020, it was not possible to purchase a medicinal product online on the territory of the Russian Federation due to the lack of a regulatory legal framework regulating such a mechanism. However, at the moment, the relevant legislation has entered into force, regulating in detail the sale of medicines in a remote format. Taking into account the presented circumstances, it seems to us that the issue of studying new legislative acts in the field of remote sale of medicines on the territory of the Russian Federation is largely being updated. The subject of the article is the mechanism of legal regulation of remote sale of medicines in Russia. The purpose of the study is to identify the problems of legal regulation of the process of remote sale of medicines in the Russian Federation at the present stage. This research is based on a combination of groups of classical general scientific methods (induction, deduction, analysis, synthesis) and a number of special methods of scientific cognition applied directly within the framework of legal science (formal legal, comparative legal and others). Within the framework of the presented article, the authors carried out a conceptual analysis of the features of the legal regulation of the sale of medicines using remote technologies, taking into account the latest changes in legislation. The specifics of remote trade in prescription and over-the-counter drugs, as well as the peculiarities of labeling of medicines on the territory of the Russian Federation, are analyzed. As a result of a comprehensive study of current trends in regulatory regulation and justification of possible methods for improving the systems for issuing electronic prescriptions, as well as mandatory labeling of medicines, a conclusion is made

about the possibility of further development of remote trade in medicines in the Russian Federation.

Keywords

remote sales, trade, e-commerce, medicines, electronic prescription, prescription and over-the-counter delivery of medicines, regulatory framework, COVID-19, pandemic

For citation: Kornienko A.S., Neretina N.G. Legal Basis for Remote Sale of Medicines in the Russian Federation. *Legal Issues in the Digital Age.* 2021, no. 4, pp. 98–113. DOI: 10.17323/2713-2749.2021.4.98.113.

Introduction

The COVID-19 pandemic has dramatically affected all spheres of public life without any exception. Among other things, it has determined the key regulatory trends in various areas during the pandemic and post-pandemic period. The modernization process in the Russian legal institutions included a number of major steps. First of all, the legislation on the sanitary and epidemiological welfare of the population has been urgently amended. It should be noted that these amendments led to the introduction and enforcement of fines for violating a high-alert regime, specifically for walking around town without reasonable grounds. Secondly, the rules regulating remote sales of medicines were modified. While the period before 2020 saw no legislative developments in this area, the acute phase of the coronavirus pandemic necessitated an urgent introduction of online technologies, which would allow to minimize face-to-face contacts and reduce the spread of COVID-19, thus helping to save people's life and health. Thus, introduction of remote sales of pharmaceuticals primarily was discussed at the State Duma level. It was proposed to make an appropriate amendment to the Federal Law providing for the possibility to sell OTC medications online from 1 July 2020 and prescription drugs — from 2022. Furthermore, it was proposed to introduce an additional legal novelty and authorize online sales of other pharmacy goods [Belova O.A., 2021:109]. In this context, it means mostly dietary supplements, medical foods, first-aid products and other medical goods.[1]

[1] Isaev A.K. Remote Pharmaceutical Sales. Available at: https://rg.ru/2019/11/12/isaev-torgovlia-cherez-internet-sdelaet-lekarstva-bolee-dostupnymi.htm (accessed: 20.11.2021); Vukolova T. Remote Sales of Medicines. Available at: https://zakon.ru/blog/2020/03/19/distancionnaya_torgovlya_lekarstvami (accessed: 20.11.2021)

The described trend in the improvement of the established legal practices continued and led to a number of important developments.

This change in the basic paradigm brought about further modification of the legislation: in March 2020 the President signed the Decree regulating general principles of the online trade in pharmaceuticals; in April an appropriate law was adopted (it should be noted that this regulation primarily had a clear delegatory character, i.e. enabling the Government to perform certain activities) [Egorova A.V., 2021: 47]. As was pointed out by T. Vukolova in her article, "following the adoption of the draft after the first reading, the legislative procedure was suspended for unknown reasons".[2] As a result, the original amendment timeframes were protracted over nearly three years instead of several months. Only some of the basic principles of the online trade in medications were adopted in May.

So, one can see a certain speedup in the process of transition to on online trade in medications: after the respective President's request, the draft considered by the Duma for nearly three years was adopted just within two weeks.

From a brief overview of the processes observed in the Russian legislation and economy, we'll pass on to a more detailed examination of the innovations triggered by the Presidential Decree No 187 "On *Retail Trade* in *Drugs* for Medical Use"[3].

The above decree served as a basis for other laws adopted two weeks later, namely: Federal Law No 105-FZ "On Amending Article 15.1 of the Federal Law on Information, Information Technologies and Protection of Information and the Federal Law on Circulation of Medicines"[4].

Having considered general provisions regulating pharmaceutical trade issues, let us turn to major specific aspects, which have a direct impact on the everyday life of Russian citizens. We'll examine how medical prescriptions are issued, whether the related paperwork can be done online, how OTC medications and prescription drugs are dispensed as well as what

[2] Vukolova T. Remote trade in medications. Available at: https://zakon.ru/blog/2020/03/19/distancionnaya_torgovlya_lekarstvami (accessed: 20.11.2021)

[3] Presidential decree of March 17, 2020 № 187 "On Retail Trade in Drugs for Medical Use". Available at: http://publication.pravo.gov.ru/Document/View/0001202003170037 (accessed: 20.11.2021)

[4] Federal Law No 105-FZ "On Amending Article 15.1 of the Federal Law on Information, Information Technologies and Protection of Information and the Federal Law on Circulation of Medicines". Available at: http://publication.pravo.gov.ru/Document/View/0001202004030060 (accessed: 21.11.2021)

requirements are imposed on e-commerce businesses in accordance with the Resolution of the Russian Government and other bylaws[5].

1. Regulation of Procedures for Issuing Medical Prescriptions

At present, there are two major procedures for issuing medical prescriptions envisioned by the active legislation of the Russian Federation. A citizen of the Russian Federation can obtain a prescription written on a standard form during his/her visit to a medical institution. Alternatively, one can obtain a medical prescription in an electronic form.

Legal grounds for prescribing medications in the Russian Federation are contained in the Federal Law No. 242-FZ of July 21, 2014 "On Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns the Application of Information Technologies in Healthcare"[6].

In accordance with this law, prescriptions for narcotic drugs or psychotropic substances shall be issued on standard official paper forms or — on condition of the patient's (or his/her legal representative's) prior consent — in the form of e-documents with an enhanced encrypted and certified digital signature of the person responsible for issuing the respective prescriptions in a given medical institution [Gorshkova V.M., Streltsov R.S., 2021: 49].

Furthermore, the approach to legal interpretation of the term "prescription" underwent a transformation. Currently, a prescription is understood to be a medical document, which has an established form and contains information about the prescribed pharmaceutical for medical use. It is issued by medical professionals with a view to enable patients to get the necessary medication from a pharmacy. It can be a standard written prescription or an electronic document. In the latter case, prior consent of the patient or his/her legal representative is required. As was noted by L.M. Ibragimova,

[5] Resolution of the Government of the Russian Federation No 697 of May 16, 2020 "On adoption of the Rules for issuing permits for the remote (distance) retail sale of medicines for medical use, as well as implementation of such trade and delivery of such medicines to citizens, and amending certain acts of the Government of the Russian Federation concerning the retail trade in medicines for medical use." Available at: http://publication.pravo.gov.ru/Document/View/0001202005180035 (accessed: 22.11.2021)

[6] Federal Law No. 242-FZ of July 21, 2014 "On Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns the Application of Information Technologies in Healthcare". Available at: http://publication.pravo.gov.ru/Document/View/0001201707300032 (accessed: 22.11.2021)

the term is also applicable "to standard paper medication forms containing prescription of pharmaceutical preparations for veterinary use" [Ibragimova L.M., 2021: 935].

The Unified State Healthcare Information System (further on referred to as USHIS) is an important element of the mechanism whereby prescriptions for medications are issued. USHIS contains the data reflected in the federal information systems, data on medical organizations (with the exception of medical organizations subordinate to the Federal Government bodies whose line of responsibilities involves military or equal-status service in accordance with Federal laws); data on medical documentation, which does not allow to determine patients' health condition; statistical data, etc. [Karonsky E.V., 2021: 255].

In the context set by the Federal law, the Ministry of Health of the Russian Federation drafted two ministerial orders, which provide a more detailed description of different prescription formats.[7]

Let us consider major provisions of the regulations issued by the Russian Health Ministry related to prescription of pharmaceutical preparations.

First and foremost, all the information about the medication prescribed (i.e. name, dosage, administration and application techniques, duration of treatment, justification for prescribing a given preparation) should be reflected in the patient's medical records. A prescription is issued either on a special printed medication form or as an electronic document (in the latter case, prior consent of the patient or his/her legal representative is required) [Magomedov A.M., 2020: 61].

Electronic prescriptions for narcotic drugs or psychotropic substances must be signed with an enhanced encrypted and certified digital signature of a physician, paramedic or maternity nurse (provided the above medical staff members have the authority to issue respective prescriptions).[8]

---

[7] Order of the Ministry of Health No 4n of January 14, 2019 "On Approval of Procedure for Prescription of Medications, Prescription Forms, and Procedure for Completion, Registration and Storage thereof". Available at: http://publication.pravo.gov.ru/Document/View/0001201903270029 (accessed: 22.11.2021); Order of the Ministry of Health No 198n of March 19, 2020 "On temporary procedure for the organization of work of medical organizations for the purpose of implementing measures for prevention and decrease in risks of spread of new coronavirus infection COVID-19". Available at: http://publication.pravo.gov.ru/Document/View/0001202003190038 (accessed: 22.11.2021)

[8] Federal Law № 63-FZ of April 6, 2011 "On Electronic Signature". Available at: https://base.garant.ru/12184522/ (accessed: 22.11.2021)

Furthermore, the ministerial order specifies that electronic prescriptions can be issued on condition that the use of e-prescriptions was approved on this constituent territory by the respective regional authorities.

If a patient is discharged from the hospital following inpatient care, he/she receives a prescription for further treatment issued upon a decision of the head of the hospital in electronic or paper form (alternatively, the required medications can be given to the patient at discharge for a period of further outpatient treatment not exceeding 5 days)[9].

The document is drawn in the name of the patient for whom the medication is prescribed. Prescriptions in an electronic form are completed automatically by the information system of the respective constituent entity of the Russian Federation. It is mandatory to document the issuance of each prescription in medical records [Krasilnikov E.F., Nikishin A.F., 2019: 218].

It is prohibited to issue prescriptions in the absence of appropriate medical grounds. Besides, it is absolutely inadmissible to include references to unregistered medications in the prescriptions. A unified set of requirements regulates the procedure for completing all types of prescriptions. Every prescription contains the following information: composition of the pharmaceutical preparation in Latin, dosage, how often and when the medication should be taken (in the morning or in the evening, duration of treatment, compatibility with the diet) [Kugach V.V., Davidovich E.I., 2017: 94]. As far as a time limit on the prescription is concerned, prescriptions of type 148-1/u-88 are valid for fifteen days and prescriptions of type 148-1/u-04(l), for thirty days from the date of issuance. If the prescription validity period is one year, it should bear a "Specialized prescription" mark as well as clear indication of the length of the validity period, and time intervals at which the medication can be dispensed. The obtained prescription is certified with a signature and stamp of the medical professional, and stamp of the medical organization. If a prescription is issued in e-form, it should be certified with enhanced digital signature. Unduly completed prescriptions are deemed invalid[10].

Thus, it should be noted that the system for issuing prescriptions in electronic form can work only if the regional authorities enact the appropriate legislation. Once they have done so, the authorities of constituent

[9] Order of the Ministry of Health and Social Development № 110 of February 12, 2007 "On the procedure for issuing prescriptions for pharmaceutical preparations, medical products, and specialized medical foods". Available at: https://base.garant.ru/12153254/ (accessed: 22.11.2021)

[10] Ibid.

entities of the Russian Federation are obliged to comply with the requirements set out in the Order of the Russian Health Ministry. However, if the regional authorities abstain from a decision to introduce electronic prescriptions, the above ministerial order is applicable only to the issuance of prescriptions in paper form.

To date implementation of the electronic prescription program is underway only in a few constituent entities of the Russian Federation. For example, the Unified *Medical Information* and *Analysis System* introduced in Moscow contains all types of prescriptions[11]. Beside Moscow, the system was implemented in a number of constituent entities, namely: Moscow Region, Saint Petersburg, Vladimir, Sakhalin, Omsk, Belgorod, and Astrakhan Regions[12].

As was pointed out earlier, the COVID-19 pandemic is making its amendments in the field of pharmacy prescription regulations. In particular, a new rule came into force in the Russian Federation starting from March 19, 2020. According to this rule, heads of medical institutions should make it possible for the patients to get electronic prescriptions while coronavirus infections continue to spread[13].

Furthermore, in line with another adopted additional rule, patients with chronic diseases are eligible to receive a prescription with a validity period extended up to three months. This means that patients undergoing regular medical check-up can obtain medications without a necessity to visit an out-patient clinic. In these cases, physicians are recommended to a medical check-up in a remote mode: namely, make regular telephone calls, ask questions about their health condition, and, if necessary, adjust treatment.

Thus, as one can see, prescriptions can be issued in different ways, i.e. via an in-person or remote mode. As far as electronic prescribing is concerned, it should be noted that this practice exists virtually in all EU countries, the USA, and the UK [Bermejo Vicedo T., Delgado Tellez de

[11] Unified Medical Information and Analysis System operates within the framework of the "Information City" Programme approved by Moscow Mayor Sergey Sobyanin in 2011. Available at: https://www.mos.ru/dit/documents/normativnye-pravovye-akty-goroda-moskvy/view/61220/ (accessed: 23.11.2021)

[12] An electronic drug prescription. Available at: https://www.provrach.ru/article/16305-elektronnyy-retsept-na-lekarstva-21-m10-12 (accessed: 23.11.2021)

[13] Order of the Ministry of Health No 198 n of March 19, 2020 "On temporary procedure for the organization of work of medical organizations for the purpose of implementing measures for prevention and decrease in risks of spread of new coronavirus infection COVID-19". Available at: http://publication.pravo.gov.ru/Document/View/0001202003190038 (accessed: 24.11.2021)

Cepeda L., Navarro Cano P., Vázquez Martínez C., Zamarrón Cuesta I., Morejon Bootello E., Balsa Barro J., 2005: 173-181]; [Fry E., Schulte F., 2019]; [Goundrey-Smith S., 2012: 22–41]; [Jolly R., 2011–2012: 1–51][14]. Notably, the EU has active rules envisioning a functional mechanism for a cross-border exchange of electronic prescriptions. In essence, this mechanism works as follows: a national of Estonia, Finland, Luxembourg, Czech Republic, and Croatia moving from country to country and visiting local pharmacies can refill prescriptions issued in the country of his/her permanent residence. It is planned that by the end of 2021 this system based on EU Directive 2011/24 will unite at least 22 states[15]. Those who design the system are aiming to integrate not only prescription data, but discharge summary information, too. The latter is fairly important since it concerns allergic reactions, therapy received, potential diseases, and previous surgical interventions [Shakel N.V., Ablameiko A.S., 2020:24].

At the same time, analysis of the regional practice of health care workers in the Russian Federation shows that e-document workflow, despite its official introduction, is not used in everyday medical practice. The data transmission system developed in 2017 is not fully functional, since it has not been fine-tuned in an appropriate manner. At the same time, in most cases implementation of the e-document workflow was initiated by the regional authorities[16].

2. Legal Grounds for Coding Medicines

The instructions of the President of the Russian Federation of 4 February 2015 triggered the development of a specialized system for monitoring

[14] Bermejo Vicedo T.,, Delgado Tellez de Cepeda L., Navarro Cano P., Vázquez Martínez C., Zamarrón Cuesta I., Morejon Bootello E., Balsa Barro J. Implantación de un sistema de prescripción electrónica asistida aplicada a la nutrición parenteral en un hospital general // Scielo. 2005, no. 3, pp. 173–181; Fry E., Schulte F. Death by a Thousand Clicks: Where Electronic Health Records Went Wrong // Fortune. 2019. March 18. Available at: https://khn.org/news/death-by-a-thousand-clicks/ (accessed: 24.11.2021); Goundrey-Smith S. History and Context of Electronic Prescribing in the US and UK. In: Principles of Electronic Prescribing. Chapter 2. Cert Clin Pharm, MRPharmS, SGS Pharma Solutions. Chedworth (UK), 2012, pp. 22-41; Jolly R. The e health revolution — easier said than done // Research paper. 2011–2012. no. 3, pp. 1–51.

[15] Directive of the European Parliament and European Council 2011/24/EU of March 9, 2011 on the application of patients' rights in cross-border healthcare. Available at: https://base.garant.ru/70161772/ (accessed: 25.11.2021)

[16] Gelzin I. What's the arrangement of the system for electronic prescription management? Available at: https://www.kmis.ru/blog/kak-ustroena-sistema-vedeniia-bezbumazhnykh-retseptov (accessed: 25.11.2021)

the flow of drugs from manufacturers to consumers (via barcoding). It was declared that the main goal of the system is to ensure effective pharmaceutical quality control and combat adulteration of medications.

Several interrelated tasks have to be accomplished to make it possible to effectively implement such a system:

preventing low-quality, adulterated, and counterfeit medications from entering the health market, and possible recall thereof;

prevention of inefficient expenditure, cutting budget spending;

control over targeted flow of medications purchased with public money;

efficient planning, and pharmaceutical stock management at all levels.

It was implied that such a system would be useful for all Russian nationals as well as to members of the business community. In particular, this assumption was substantiated by two reasons. For one thing, consumers get an evident advantage since they are given an opportunity to do a quick check and efficiently verify the legality of the medication they intend to buy.

Secondly, entrepreneurs also benefit from the program. Their potential costs are reduced due to increased efficiency of logistic management. Pharma business also has a lower level of missed profits related to counterfeit and falsified products; pharmaceutical market becomes more competitive, and oriented towards Western healthcare standards [Kudryashova M.N., Sudakova O.A., 2021: 86].

Despite a number of positive developments, the instruction of the President of the Russian Federation was fulfilled with a considerable delay. The necessary legal framework was developed only in 2018-2019.

A number of representatives of the pharmaceutical industry were skeptical about the possibility of effective implementation of the barcoding program in 2020. They pointed out that production process at the appropriate enterprises has been substantially modified during the coronavirus pandemic, and quite a few employees are put on leave. This led them to the conclusion that the time frame of the program should be extended.

However, the Government did not accept the reasoning of the pharmaceutical industry representatives. In May 2020, it introduced conceptual changes to the Medical Licensing Regulation by supplementing the list of licensing requirements for medical organizations. Since then, entering data on pharmaceutical preparations into the Federal State Information System

has become a mandatory licensing requirement for medical organizations with a view to facilitate access to pharmaceutical therapy[17].

In other words, since 1 July 2020 entering data on pharmaceutical preparations into the Federal State Information System has become a mandatory licensing requirement for medical organizations which would greatly facilitate patients' access to pharmaceutical therapy [Taranik M., Savkina A., Dudareva V., 2020: 38].

Thus, coding of medicines is seen as a tool, which would help to create a unified database covering all licensed pharmaceuticals eligible to be sold at pharmacies.

It's quite clear that such a model includes the following sequence of actions: firstly, any national of the Russian Federation receives an electronic prescription; secondly, he/she shows a QR-code at a convenient pharmacy of his choice; thirdly, he/she receives the appropriate medication on the basis of this QR-code; fourthly, at any time and without outside help consumers can check compliance of the obtained product with legal requirements.

3. Prescription and Non-Prescription Medication Sales

Analysis of the presented legislative information suggests that federal legislators failed to provide for the possibility to sell prescription medications in a remote mode.

So, Russian citizens have just two options. The first option is to go to a pharmacy to get the necessary medication or ask one of the relatives to do so; secondly, one can apply to a healthcare professional who has not only to issue a prescription medicine, but also (if need be) deliver it to patient's home (the latter rule applies only to persons who are officially under quarantine due an infectious disease dangerous to the public)[18].

[17] Resolution of the Government of the Russian Federation № 688 of May 15, 2020 "On Amending Article 5 of the Medical Licensing Regulation (except for the aforementioned activities exercised by the medical and other organizations affiliated to a private healthcare system on the territory of the Skolkovo Innovation Center)". Available at: http://publication.pravo.gov.ru/Document/View/0001202005180024 (accessed: 25.11.2021)

[18] Order of the Ministry of Health No 198n of March 19, 2020 "On temporary procedure for the organization of work of medical organizations for the purpose of implementing measures for prevention and decrease in risks of spread of new coronavirus infection COVID-19". Available at: http://publication.pravo.gov.ru/Document/View/0001202003190038 (accessed: 26.11.2021)

It stands to reason that personal visits to a pharmacy would be the most popular way of getting prescription medications. In such cases, the procedure for dispensing medications is regulated by Order of the Russian Health Ministry No 403 of 11 July 2017 "On adoption of rules for dispensing pharmaceutical preparations for medical use including immunobiological drugs by pharmacies and sole entrepreneurs with a pharmaceutical license". It is set out in this document that prescription medicines can be dispensed only by pharmacies and pharmacy branches as well as sole entrepreneurs (however, the latter are not eligible to sell narcotic drugs and psychotropic substances)[19].

Unduly completed prescriptions must be registered in a special logbook. Each entry should contain information about the type of deviation from the rules, full name of the person who issued the prescription, and measures taken by the pharmacist.

Improperly completed prescription is marked with the stamp "Not Valid" and returned to the owner. Each impropriety is reported to the head of the respective medical institution [Romanova A. E., 2019: 123].

Thus, prescription drug sale involves the following important stages:

a physician issues a prescription on the basis of the collected information about the patient's condition;

this prescription is shown to a pharmacist (sometimes, where narcotic drugs or psychotropic substances are involved, a personal identification document should be produced along with the prescription);

the pharmacist closely examines the prescription shown by the customer checking the its correctness and major identifiers, and interprets what is written in Latin);

if the prescription is written correctly, the pharmacist dispenses medication. If the prescription is written improperly, the pharmacist refuses to dispense medication.

Summing up the above, we are witnessing a situation where the possibility of online prescription medicines ordering and delivery is completely discarded.

[19] Order of the Ministry of Health of the Russian Federation No 403 of July 11, 2017 "On adoption of rules for dispensing pharmaceutical preparations for medical use including immunobiological drugs by pharmacies and sole entrepreneurs with a pharmaceutical license". Available at: http://publication.pravo.gov.ru/Document/View/0001201709110035 (accessed: 26.11.2021)

Sale of non-prescription medications is regulated by several major by-laws setting out the following rules: while selling medications the pharmacist should inform the customer about the main issues related to its use; medications should be stored at the proper temperature, and its shelf life should comply with all regulatory requirements [Streltsov R.S., Gorshkova V.M., 2021: 33].

As far as a remote trade in non-prescription medications is concerned, the major piece of legislation in this field is represented by the Rules for issuing permits for the remote retail sale of medicines for medical use and delivery of such medicines to citizens. [20]

Remote retail trade in non-prescription medications is conducted by pharmacies having a special license under the stipulation that this license was issued not earlier than a year ago. Furthermore, an eligible retail pharmacy must meet a number of requirements: it should have at least 10 locations on the territory of the Russian Federation where its pharmaceutical activities are conducted; within company premises, it should set up spaces for storing ready-to-ship products; it is also necessary to have a website or a mobile application; one more prerequisite is to have one's own and adequately equipped courier service (e.g. special pharmaceutical containers to ensure safe delivery of temperature-sensitive medicines); availability of the electronic fund transfer system or mobile points of sale [Turchenkova E.S., Kovalenko N.V., 2021: 208].

The Rules for issuing permits for the remote retail sale of medicines for medical use and delivery of such medicines to citizens stipulate that the following information should be made available on the pharmacy's website and mobile application: full company's trade name, Primary State Registration Number (OGRN), Tax Payer Id. Number, addresses, graphic reproduction of the license, graphic reproduction of the permit for remote trade, working hours, full information about the medication ordering service, and enquiry service, information about the medications in stock (as well as the data on the staff member responsible for posting on the Internet all the information about the medication); information concerning medication return issues; data on the authority, which exercises control over

[20] Resolution of the Government of the Russian Federation No 697 of May 16, 2020 "On adoption of the Rules for issuing permits for the remote (distance) retail sale of medicines for medical use, as well as implementation of such trade and delivery of such medicines to citizens, and amending certain acts of the Government of the Russian Federation concerning remote retail trade in medicines for medical use." Available at: http://publication.pravo.gov.ru/Document/View/0001202005180035 (accessed: 26.11.2021)

retail sales of the medication; and customer's liability [Cherkasova E.S., 2021: 63].

Furthermore, the Rules contain a provision, which stipulates that delivery of the ordered products is performed either by the pharmacy staff or other person on the basis of an agreement specifying the liability of each side, operating procedures, and responsibility. Delivery of temperature-sensitive medications can be done only using temperature controlled vehicles (alternatively, special packaging can be used) [Yatsenko A.M., 2021: 147].

Conclusions

Currently the legal framework concerning remote trade in medicines in the Russian Federation is far from perfect as evidenced by multiple legal loopholes.

The Parliament lacks supervisory powers. We think that ideally granting the Russian Government the right to organize the system of remote pharmaceutical trade should have been accompanied with vesting supervisory powers in the legislative body. In our view, the Parliament as a representative body is obliged to check how active legal rules are enforced and implemented. Specifically, this responsibility can be devolved to the relevant committee of the State Duma or Federation Council. The absence of supervision, as well as lack of detail in some of the regulations, undermine innovative potential of the online trade.

Advertising on the pharmacy websites. While many foreign countries have legal standards for website design, and requirements concerning marketing of pharmaceuticals on the Internet (e.g. it is not allowed to use colour highlighting of specific prices for medications), in Russia similar rules have not yet been developed. As to the acting Federal Law "On Advertising", it has multiple gaps and inaccuracies. Judging by the current trends in Russian legislative activities, the possibility of adopting foreign experience seems highly unlikely. And this means that for a long time (until the first occurrence of serious and systemic violations) the appropriate regulatory framework will be absent.

Patient-pharmacist interaction. Foreign legislation solves the problem of medication ordering and delivery in the following way: pharmacists as authorized representatives of the respective pharmacies or pharmaceutical networks are eligible to counsel customers on all major relevant issues. Accordingly, delivery of products is performed by pharmacists who bear personal responsibility for the quality of the medications provided. In Rus-

sia we observe a different situation where clients have virtually no direct contact with persons responsible for quality compliance and timely delivery which hampers the development of online medication delivery services in the Russian Federation.

Thus, the above outlined negative aspects in the field of remote trade in medications in Russia suggest that the existing system can be hardly called efficient.

References

1. Belova O.A. (2021) Topical innovations in the field of remote retail trade. *Vestnik Evroaziatskoy Akademii administrativnykh nauk* = Courier of the Eurasian Academy of Administrative Sciences, no. 2, pp. 105–107. (In Russ.).

2. Bermejo Vicedo T., Delgado Tellez de Cepeda L., Navarro Cano P., Vázquez Martínez C., Zamarrón Cuesta I., Bootello E., Balsa Barro J. (2005) Implantación de un sistema de prescripción electrónica asistida aplicada a la nutrición parenteral en un hospital general. *Scielo*, no. 3, pp. 173–181.

3. Cherkasova E.S. (2021) Transformation of the pharmaceutical market in Russia. *Aktualnye problemy i perspektivu razvitia ekonomiki: rossiyskiy I zarubezhnyi opyt* = Current issues and development prospects of the economy: Russian and foreign experience, no. 3 (35), pp. 62–67. (In Russ.).

4. Egorova A.V. (2021) Topical aspects of legislation pertaining to remote pharmaceutical sales on the territory of Russian Federation. *Sovremennye podhodu k organizatcii snabzhenia lekarstvami*=Modern Approaches to Organization of Drug Provision, vol. 8, no. 1, pp. 46–49. (In Russ.).

5. Gorshkova V.M., Streltsov R.S. (2021) Remote pharmaceutical sales as a new trend in the development of the pharma market in Russia. *Meditcinsloye pravo* = Medical Law, no. 2, pp. 48–51. (In Russ.).

6. Ibragimova L.M. (2021) E-commerce in the pharmaceutical industry. *Innovatccii. Obrazovanie. Nauka*=Innovations. Education. Science, no. 32, pp. 934–938. (In Russ.).

7. Jolly R. (2012) The e-health revolution — easier said than done. Research paper, no. 3, pp. 1–51.

8. Karonsky E.V. (2021) Modern forms of trade in the pharmaceutical industry. *Rossiyskiy ekonomicheskiy vestnik* = Russian Economic Bulletin, vol. 4, no. 3, pp. 254–258. (In Russ.).

9. Krasilnikov E.F., Nikishin A.F. (2019) Online reality of the developments in the Russian pharmaceutical market. *Vestnik Altaiskoy Akademii ekonomiki i prava* = Courier of the Altai Academy of Economics and Law, no. 2, pp. 217–221. (In Russ.).

10. Kudryashova M.N., Sudakova O.A. (2021) Coding of medications: theoretical and practical aspects. *Tverskoy meditcinskiy zhurnal* = Tver Medical Journal, no. 1, pp. 84–89. (In Russ.).

11. Kugach V.V., Davidovich E.I. (2017) History of an electronic prescription. *Pharma Courier*, no. 1, pp. 92–103. (In Russ.).

12. Magomedov A.M. (2020) Development of online trade in pandemic conditions. *Menedzhment, ekonomika, politika, sotciology* = MEPS: management, economics, politics, sociology, no. 3, pp. 60–65. (In Russ.).

13. Prescribing (2012) UK: Cert Clin Pharm, MRPharmS, SGS Pharma Solutions.Chedworth (UK), pp. 22–41.

14. Romanova A.E. (2019) Remote trade in pharmaceuticals as a possible novelty in the Russian legislation. *Vestnik Nizhegorodskogo gosudarstvennogo universiteta* = Courier of State University of Nizhny Novgorod, no. 3, pp. 120–124. (In Russ.).

15. Shakel N.V., Abramenko A.C. (2020) Foreign experience in implementing electronic healthcare systems: critical analysis. *Zhurnal mezhdunarodnogo prava i mezhdunarodnykh otnosheniy* = Journal of International Law and International Relations, no. 92–93, pp. 20–26. (In Russ.).

16. Streltsov R.S., Gorshkova V.M. (2021) Problems and perspectives of online trade in medications on the pharmaceutical market of the Russian Federation. *Nauka Krasnoyarya* = Science of Krasnoyarye, vol. 10, no. 4, pp. 30–34. (In Russ.).

17. Taranik M., Savkina A., Dudareva V. (2020) How to start working with medications within the “Coding” information system. *Kachestvo upravlenia v zdravookhranenii* = Quality Management in Healthcare, no. 3, pp. 37–39. (In Russ.).

18. Turchenkova E.S., Kovalenko N.V. (2021) Online pharmacy as a new form of medication sales. *Biznes. Obrazovanie. Pravo* = Business. Education. Law, no. 1 (54), pp. 204–210. (In Russ.).

19. Yatsenko A.M. (2021) Regulatory issues of remote drug sales. Uchenye zapiski tambovskogo filiala rossiyskogo obedinenia molodukh uchenukh=Scholarly notes of the Tambov Branch of the Russian Union of Young Scientists, no. 22, pp. 143–150. (In Russ.).

Information about the authors:

A.S. Kornienko — Candidate of Sciences (Economics), Assistant Professor.

N.G. Neretina — Candidate of Sciences (Sociology), Assistant Professor.

The article was submitted 22.09.2021; approved after reviewing 12.11.2021; accepted for publication 26.11.2021.

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4.

Research article
УДК 343+341.45
DOI: 10.17323/2713-2749.2021.4.114.129

On the Definition, Legal Essence and Classification of Electronic Information Used Within the Framework of International Cooperation in Criminal Matters

Kirill Klevtsov

MGIMO University, Moscow, Russia, klevtsov001@gmail.com, https://orcid.org/0000-0003-2918-175X

Abstra

The article is devoted to the analysis of such a complex and multifaceted legal phenomenon as „electronic information“. The aim of the research is to define the concept and legal nature of such information. The analysis is based on materialistic dialectics, legal hermeneutics, special and comparative legal methods, a sociological approach and a forecasting method. The study shows that the doctrine and practice lacks a unified approach to understanding electronic information in criminal cases, often the concept of „electronic information“ is confused with „electronic evidence“, while losing sight of its criminal procedural application. Author comes to the conclusion that there is no legislative definition of the concept of “electronic evidence” and it is still possible to operate with the term “electronic information” today, taking into account its cross-disciplinary purpose, respectively, the author’s definition of this concept is proposed. In addition, an attempt was made to determine the types of electronic information in criminal cases, including those requested in the framework of international cooperation, namely, the provision of mutual legal assistance. As an empirical basis for the study, we used the materials contained in the Practical Guide for Requesting Electronic Evidence from Other Countries, prepared jointly by the UN Office on Drugs and Crime, the Executive Directorate of the UN Security Council Counter-Terrorism Committee and the International Association of Prosecutors in collaboration with the EuroMed Justice programs and Euromed Police.

Keywords

electronic information, criminal cases, electronic evidence, international cooperation

For citation: Klevtsov K.K. On the definition, legal essence and classification of electronic information used within the framework of international cooperation in criminal matters. Legal Issues in the Digital Age. 2021, no. 4, pp. 114–129. DOI: 10.17323/2713-2749.2021.4.114.129.

To date, there is no clear understanding both at the doctrinal level and in judicial practice of what "electronic information" is and what is its place in the legal system, including in criminal law. This problem creates serious difficulties in using electronic data as evidence in criminal cases. This seems to be due to the lack of a clear understanding of the comprehensive term "information", which also needs to be clarified taking into account modern realities.

Today's time at the doctrinal level is defined as the "information era" [Churinov N.M., 2002: 10–15], [Raenko S.I., 2013: 189–194], since information [informatio][1] was often of interest both to scientists and to society as a whole. However, until now in philosophy and in other sciences there is no unified approach to understanding the concept of information.

In this regard, the statement of V. Polonskiy, who believes that "the state of the conceptual and terminological apparatus of science allows one to judge the degree of development of the theory corresponding to it, to highlight the various aspects, relationships of real objects and the variety of cognitive tasks ..." [Polonskiy V.M., 1999: 16].

For example, explanatory dictionaries of the Russian language define information as (1) information about the surrounding world and the processes occurring in it, perceived by a person or a special device; and (2) messages informing about the state of affairs, about the state of something.[2] A similar definition is found in jurisprudence dictionaries.[3]

However, this concept is considered differently, depending on the relevant areas of science, which led to the lack of a unified approach. On this score, as it seems to us, V. Vasyukov that this situation is caused by the complex nature of relations based on the theoretical arguments of many sciences: computer science, communication theory, information theory, cybernetics, philosophy, semiotics, information dynamics (the science of open information systems), information science (the science of obtaining, storing and transmitting information for various sets of objects), etc.

[1] From Latin "understanding".

[2] See Ozhegov S.I. (2006) Explanatory dictionary of Russian language. Moscow: Institute of Russian language, RAS; Ushakov D.N. (2014) Explanatory dictionary of modern Russian language. Moscow.

[3] See e.g. Borisov A.B. (2010) Extended legal dictionary. Moscow: Knizhny mir.

[Vasyukov V.F., 2020: 43–44]. From the point of view of informatics, it is a primary concept by analogy with "matter", "energy", as a result of which it cannot be defined through simple categories that have clear boundaries [Bauer F.L., Goos G., 1990: 18]. At the same time, in philosophy, according to the general rule, two theories have been formed — functional and attributive. The first is understood as the fact that information is a product of humanity, therefore, it is cognized only by an individual. According to the second concept, it is matter, along with space and time. [Ursul A.D., 1975: 29], [Afanasyev V.G., 1980: 238].

Today there is a legislative definition of information. According to para. 1 of Art. 2 of the Federal Law of 27.07.2006 No. 149-FZ "On information, information technologies and information protection", information means information any messages or data regardless of the form of their presentation.[4] In the criminal procedure doctrine, attempts have also been made to define information in the context of the theory of evidence. So, for example, V.Ya. Dorokhov meant by it "any information used as evidence in criminal proceedings, having a signal nature" [Dorokhov V.Ya., 1964: 108–117]. At the same time, Professor A.A. Davletov pointed out that information is an element of retrospective cognition, a means by which the subject of cognition establishes the presence or absence of a fact. [Davletov A.A., 1991: 24].

We share the opinion of A.I. Zazulin that in criminal procedural and criminalistic law, participants often encounter analog[5] or discrete[6] information, since it is itself perceived through interrogation, testimony of participants, perception of traces of crime, and the results are denounced either in documents containing the results of operational investigative activities or in the protocols of investigative and judicial actions. [Zazulin A.I., 2018: 79]. At the same time, a special group is made up of electronic information, which has specific features that differ from the ordinary one. In a number of works on criminal procedural law and forensic science, there are similar terms, namely: "machine information"[7], "computer information", "digital information".

It should be noted that the term "machine information" in the criminal law sciences and in the course of the fight against crime, as a general rule,

[4] Collection of Legislative acts of Russian Federation, no. 31 from 31.07.2006 (part I) Art. 3448

[5] An analog signal is a human speech or an image in a photograph.

[6] This is the text, which consists of letters, symbols.

[7] For example, I. Karas proposes to understand it as information circulating in cyberspace, recorded on a physical medium, in a form accessible to the perception of a computer, or transmitted through telecommunication channels [Karas I.Z., 1990: 40].

has been abandoned. This seems to be due to the use of the concept of "computer information" or "computer data"[8] in many legal documents.[9] At the same time, despite the existing international legitimation of this concept, there are still discussions in scientific circles regarding the definition of this phenomenon.

So, A. Kasatkin believes that computer information is factual data that are processed by a computer and obtained at its output in a form that can be perceived by a computer or a person [Kasatkin A.V., 1997: 26]. At the same time V. Krylov understands by it the information, knowledge or a set of commands (programs) intended for use in a computer or controlled by it, located in a computer or on a machine carrier [Krylov V.V., 1997: 27]. A somewhat vague definition, as we see it, is given by N. Zigura. In his opinion, computer information is information that exists in digital form on a physical medium [Zigura N.A., 2010: 28].

Each of the above definitions undoubtedly reflects certain characteristic features of the phenomenon we are considering. However, it is still worth pointing out that the concept of "computer information" in relation to the doctrine of criminal law and criminal procedure has some distinctive features that, it seems, must be taken into account when defining it. At the same time, one should ask an important question, both from a theoretical and practical point of view. The information in smartphones, smart watches, tablets, in the legal sense, refers to computer information, despite the fact that in everyday life these media are a kind of computers.[10] The

[8] Paragraph "b" of Article 1 of the Convention on Cybercrime ETS No. 185, adopted in Budapest on November 23, 2001 (hereinafter — the Budapest Convention), states that "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

[9] According to paragraph "b" of Art. 1 of the Agreement of the Commonwealth of Independent States on combatting crimes in the field of information technology, concluded in Dushanbe, on September 28, 2018, under the computer information is understood the information that is stored in the memory of a computer, on machine or other media in a form accessible to the perception of a computer, or transmitted through communication channels.

Note to Art. 272 of the Criminal Code of the Russian Federation defines this information as information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing and transmission.

It is worth paying attention to the recently introduced operative investigation measure — "obtaining computer information", provided for in paragraph 15 of Art. 6 of Federal Law from 12.08.1995 "On operative investigation activity" (Collection of Legislative acts of Russian Federation (1995), no. 33, Art. 3349).

[10] For example, the „computer" https://en.wikipedia.org/wiki/Computer (accessed 01.12.2021).

information contained in digital cameras, video recorders, robotic vacuum cleaners, etc. is ambiguous in its legal nature. Unfortunately, Russian legislation does not give an unambiguous answer to these questions, as a result of which, we believe, this negatively affects law enforcement.

For example, due to the lack of a detailed procedure for conducting operative investigation measures in the Federal Law "On Criminal Investigation" and the abundance of closed documents, difficulties arise in obtaining information transmitted through instant messaging systems, namely with the help of what type of operational-search measures such data can be obtained? By obtaining information from technical communication channels (clause 11 of article 6) or obtaining computer information (clause 15 of article 6)? To date, this issue remains controversial, despite individual attempts to regulate it in departmental legal acts. In this regard, for example, V. Mescheryakov considers it necessary to abandon the term "computer information", and suggests replacing it with the term "digital object" [Mescheryakov V.A., 2004: 163]

However, some scholars suggest using the term "digital information", taking into account the variety of forms in which such information can exist and be transmitted [Walker C., 2001: 87–88]. For example, N. Ivanov believes that digital information is information recorded on machine media, or transmitted in space in the form of discrete signals — regardless of their physical nature [Ivanov N.A., 2013: 97]. In turn, S. Kushnirenko understands by it information presented in the form of a sequence of numbers available for input, processing, storage, transmission with the help of technical devices [Kushnirenko S.P., 2006: 39]. Some analysts went even further and proposed an original term, considering it an analogue of digital information. This is "information presented in electronic form, which is recorded on machine media, regardless of their physical nature" [Kuvychkov S.I., 2016: 60].

In order not to get bogged down in the discussion, we consider it expedient to use the broader phrase "electronic information" that is applied in law enforcement in criminal cases.[11] Scholars operate with this term as well [Salinovsky K.V., Markelova G.Yu., 2001: 18] [Zaitsev O.A., 2019:

[11] For example, in Art. 1641 of the Code of Criminal Procedure of the Russian Federation refers to the peculiarities of the seizure of electronic media and copying information from them in the course of investigative actions, and in part 7 of Art. 185 of the Code of Criminal Procedure of the Russian Federation uses the terms "electronic messages", "messages transmitted over telecommunication networks." At the same time, the ambiguity of some formulations in these articles is noted in legal doctrine [Vasyukov V.F., 2016: 15–18]; [Shaidullina E.D., Shmeleva O. G., 2018: 44–49]; [Stelmakh V.Yu., 2021: 146–155]. Therefore, proceeding from formal logic, the following conclusion is made that this information is electronic.

42–57] [Pastukhov P.S., 2015: 127–130]. Western lawyers also choose a similar approach in most cases.[12] Electronic information includes various files that contain text, photographs, video recording, sound recording, including those transmitted through the instant messaging system, databases and programs, system files, service utilities and their protocols. Moreover, such information can be located both physically on devices and remotely (for example, in cloud storage).[13] It is obvious that such electronic information can be used in criminal procedural evidence. One of the debatable issues is also the question of the relationship between the concepts of "electronic information" and "electronic evidence". First of all, this is due to the ongoing discussions in general about the concept of evidence [Vyshinsky A.Ya., 1941], [N.V. Zhogin, 1971], [Vladimirov L.E., 2000], [Polyansky N.N., 1946].However, in Russian legislation there is a legal definition of evidence[14], according to which it consists of three elements: (1) factual data (information about facts); (2) sources of factual data; (3) methods and procedure for collecting, consolidating and verifying this factual data. [Balakshin V.S., 2002: 31].

Undoubtedly, the situation with determining the legal nature of electronic evidence is more complicated, as can be seen from the wide range of opinions expressed by lawyers on this issue. Some of them point out that evidence secured in electronic form should be classified as traditional types of evidence. For example, S. Vorozhbit, in the light of civil procedural law, writes that "depending on the type of those electronic data that have evidentiary value, that is, contain information necessary to establish the circumstances of the case, they can be attributed to written, material evidence, audio or video recordings "[Vorozhbit S.P., 2011: 8]. Others believe

[12] See: Strafprozessordnung (StPO) der Bundesrepublik Deutschland. Available at: https://www.gesetze-im-internet.de/stpo/; Code de procédure pénale de France Available at: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/ (accessed: 01.12.2021) etc.

[13] Cloud storage is a model of computer data storage in which the digital data is stored in logical pools, said to be on "the cloud". The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment secured, protected, and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Available at: https://en.wikipedia.org/wiki/Cloud_storage (accessed: 01.12.2021).

[14] According to Part 1 of Art. 74 of the Code of Criminal Procedure, evidence in a criminal case is any information on the basis of which the court, prosecutor, investigator, inquirer, in the manner prescribed by the CCP, establishes the presence or absence of circumstances to be proved in the course of criminal proceedings, as well as other circumstances relevant to the criminal case.

that electronic evidence is a special group within already existing types of evidence, as a result of which they should be given a specific status, taking into account their characteristics. For example, Yu. Sokolov proposes to fix in Art. 81 of the Code of Criminal Procedure of the Russian Federation, a separate wording that allows to recognize as material evidence also information provided in electronic form, which served as an instrument of crime or retained traces of a crime, or at which criminal actions were directed [Sokolov Yu.N., 2010: 116]. It seems that this position is controversial, since it does not differ from the current version of the above article of the Russian criminal procedure law (Article 81). Finally, the third point of view believes that electronic information is a completely new type of evidence, along with others enshrined in Part 4 of Art. 74 of the Criminal Procedure Code of the Russian Federation, since it has specific properties that make them different from other types of evidence [Zagura N.A., Kudryavtseva A.V., 2011: 30].

It should be noted that domestic law enforcement practice classifies the so-called electronic evidence as material evidence, since this is directly provided for by Art. 81 and Art. 84 of the Code of Criminal Procedure of the Russian Federation, as a result of which we share the position of the first group of scholars who classify them as traditional types of evidence. With regard to this problem, R. Okonenko correctly noted that, for example, the appearance of cameras, voice recorders and video cameras, did not lead in the practice of criminal investigation to the classification of information contained in these devices as a special type of evidence [R.I. Okonenko. 2016: 25]. It also did not lead to the emergence of new investigative actions that allowed obtaining such extraordinary evidence. Undoubtedly, it is worth recognizing that there are forensic features of obtaining such electronic information.

Professor L. Golovko discusses this in a very revealing manner. In his opinion, if the protocols of investigative and judicial actions are drawn up in electronic form, then there will be no new "type" of evidence, since the protocols will remain protocols, regardless of the form of their production (handwritten, electronic, etc.). As a result, the cited author comes to the conclusion that there is simply no need for special electronic evidence [Golovko L.V., 2019: 22–25].

Returning to individual aspects of the two previously mentioned terms, we note that some international documents operate precisely with the phrase "electronic evidence".[15] Moreover, in Western legal doctrine, similar

[15] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final — 2018/0108 (COD) // Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed: 01.12.2021); Practical

terminology is used [Moussa A.F., 2021], [Kerr O.S., 2010: 23], [Mason S., 2012: 26–27], [Mason S., 2014: 25–36]. It seems that this is determined by the difference in the legal systems of states, approaches to the definition of evidence and their legal nature. For example, in Common Law countries they use the concept of evidence in a broad sense, without attaching the Russian procedural meaning, as a result of which they legitimately add the word "electronic" to it. For example, in the USA there is no clear differentiation of evidence into types and more emphasis is placed on the formal rights of participants in criminal proceedings when collecting and using evidence in courts [Pizzi U., 21–46], [Burnham U., 2006: 207–216], [Reshetnikova I.V., 1997]. It should be emphasized that the US Federal Evidence Rules, which are a fundamental document in American evidentiary law [Rothstein P.F., 1991: 2], do not contain the concept of "electronic evidence", but use the phrase "electronically stored information".

As Professor O. Zaitsev notes, in most countries of the Continental Law, the admissibility of the use of electronic information is regulated by the general provisions of the legislation on traditional evidence [Zaitsev O.A., 2019: 50].

Without going into serious reflections on this score, we note that today, due to the lack of a normative and doctrinal unambiguous answer to the above question, the phrase "electronic information" should be used, not "electronic evidence". In confirmation of this conclusion, one can also cite the positions of domestic scientists in the field of criminal procedure.

So, M. Strogovich wrote that until the proof is not fixed procedurally, it is not worth arguing that the proof really exists [Strogovich M.S., 1986: 302]. At the same time, Professor S. Sheyfer argued that to recognize the object as evidence, i.e. to introduce it into the process is exclusively the prerogative of the investigating body, the prosecutor and the court, since it is the decision to attach the subject or document to the case that represents the final moment in the formation of evidence [Sheyfer S.A., 1981: 45–46]. Professor V. Balakshin adheres to an approximately similar position [Balakshin V.S., 2004: 94-109]. The same applies to information obtained in the framework of investigation activities, on behalf of the investigator and inquirer[16], as well as in the verification of a crime report (Art. 144 of the

guide for requesting electronic evidence across borders. Vienna: United Nations, 2019.

[16] In the manner prescribed by the Order of the Ministry of Internal Affairs of Russia No. 776, the Ministry of Defense of Russia No. 703, Federal Security Service of Russia No. 509, Federal Protective Service of Russia No. 507, Foreign Intelligence Service No. 42, Federal Penitentiary Servise of Russia No. 535, Federal Drug Control Service of Russia No. 398, Investigation Commetee of Russia No. 68 of September 27, 2013 "On approval of the instruction on the procedure for presenting the results of operative investigation activities to the body of inquiry, investigator or court."

Code of Criminal Procedure of the Russian Federation), which can be considered evidence only after their "procedural assessment". The rationale on this issue is contained in the reasoning of N. Zigura, who believes that the computer information provided by the participants in the criminal process or other persons "will be considered evidence only after the investigator recognizes it as relevant and admissible, and this will happen after reproduction, examination , drawing up a protocol of examination and satisfaction of the petition to attach the carrier of information to the case "[Zigura N.A., 2011: 131].

It follows from this that any electronic information that is de facto evidence in a specific criminal case remains just information until it is collected, verified and evaluated according to the rules of Russian criminal proceedings (Section III "Evidence and proof"). The same argument applies to electronic information in criminal cases obtained in the framework of international cooperation, which will be discussed in more detail below.

Having defined in general terms the terminology and legal nature of electronic information in criminal cases, it is worth moving on to another question that is interesting from a theoretical point of view, but not devoid of its applied purpose. This relates to the problem of the classification of electronic information. This issue was analyzed in detail in the framework of forensic research of digital traces [Meshcheryakov V.A., 2002: 103], [Volevodz A.G., 2002: 159–161], [Kozlov V.E. 2002: 91], [Krasnova L.B., 2005: 25–72], [Smushkin A.B., 2012: 43–48], [Lyanov M.M., 2020: 47–55]. At the same time, the authors of these studies did not touch upon the issues of obtaining electronic information on criminal cases in the context of international cooperation.

So, leaving out the technical and forensic aspects of electronic information, the following classification is proposed.

Depending on the stages of criminal proceedings: (a) obtaining electronic information in the framework of pre-trial proceedings (Part 2 of the CCP RF) and (b) in the course of court proceedings (Part 3 of the CCP RF). At the same time, the receipt of such information in the course of pre-trial proceedings can be both (i) at the stage of initiating a criminal case (Section VII of the CCP RF), and (ii) during the period of preliminary investigation (Section VIII of the CCP RF).[17]

Taking into account the place of its storage: (a) information physically located in the network of national servers (national information resources); (b) information held abroad (extra-territorial information).

[17] Based on the aim of the research, the author analyses exclusively the obtaining electronic information in the framework of pre-trial criminal proceedings.

By its content the electronic information can be (a) publicly available and (b) confidential, i.e. contain state or other secrets protected by law.[18]

From the point of view of the legal basis for receiving electronic information, it can be claimed on the basis of (a) national (domestic) law [19]or (b) the norms of international law.[20]

By subjects. Depending on access to electronic information, such can be (a) individuals who have an electronic storage medium on which such information is stored and who has access to it[21]; (b) the service provider;[22] or (c) the representation of the service provider in another country.

Taking into account the mechanism for obtaining electronic information, it can be classified into information obtained through (a) operational and investigative means, including in the implementation of international police cooperation (for example, police officers sent a request for assistance to law enforcement agencies of foreign states on the basis of intergovernmental agreements or through the National Central Bureau of Interpol), (b) conducting investigative actions (for example, through the sending by the investigator of a request for mutual legal assistance both to the competent authorities of a foreign state and to an entity with access to such information).

Depending on the criminal procedural fate of electronic information. Thus, the data obtained in the framework of international cooperation can

[18] In Russian legislation, such information includes (i) state secrets; (ii) trade secrets; (iii) bank secrecy; (iv) official secrets; (v) professional secrecy (for example, lawyer's, medical), etc. This classification follows from the interpretation of the provisions of the Criminal Procedure Code of the Russian Federation, the Federal Law "On Information"; Law of Russian Federation of July 21, 1993 "On state secrets"; Federal Law of July 29, 2004 "On commercial secrets"; Labor Code of the Russian Federation and various laws providing for service in law enforcement agencies; The Civil Code of the Russian Federation (for example, Art. 857), the Law of Russian Federation of February 12, 1990 "On Banks and Banking Activity", the Federal Law of May 31, 2002 "On the Advocacy and the Bar in the Russian Federation", the Federal Law of December 30, 2008 "On Audit Activity ", The Federal Law of November 21, 2011" On the basics of protecting the health of citizens "; Law of the Russian Federation of July 02, 1992" On psychiatric care and guarantees of the rights of citizens in its provision ", etc. [Popov L.L. 2010: 125–189].

[19] For example, part 4 of Art. 21 of the Code of Criminal Procedure of Russia, clause 31, part 3 of Art. 101 of the Federal Law "On Information".

[20] For example, within the framework of the Budapest Convention, the CIS Convention on Computer Crimes, etc.

[21] Such terminology is enshrined in legislation (for example, Art. 1641 of the Criminal Procedure Code. In addition, according to GOST 2.051-2013, an electronic medium is understood as a material medium used for recording, storing and reproducing information processed using a computer. Electronic information carriers can be used as independent objects (flash drives, memory cards, various removable drives, CD, etc.), and is part of other objects (servers, system units, laptops, video recorders, tablets, mobile phones, etc.).

[22] In this article, it means organizations (companies) providing Internet access services, providing access to a cable network, satellite network, social networking services and transmitting information electronically.

be recognized as (a) material evidence (Article 81 of CCP RF), (b) as other documents (part 2 of Article 84 of the CCP RF) or (c) not recognized as evidence, and returned back to the competent authorities of the foreign state.

It should be noted that within the framework of international cooperation in criminal matters, as a rule, the following types of electronic information are requested.

Basic Subscriber Information. It is the name of the subscriber and may contain information about how long the subscriber has used this particular service, as well as the IP address from which the system was first logged in.

Transactional Information (without content information) — metadata associated with the provision of services. This information includes (a) data related to the connection, traffic, or location of the communication (for example, IP address or MAC address); (b) access logs, which record the time and date of access to the service by a specific individual, as well as the IP address from which the service is accessed; (c) transaction logs, which record a product or service received by a specific individual from a supplier or third party (for example, purchase of cloud storage space).

The content. It represents the text of an email (message), blog or post, video, image or sound stored in digital format (excluding subscriber data or metadata).[23]

Thus, during the criminal prosecution by French law enforcement agencies of terrorist A., who killed two French police officers at their home, it became necessary to obtain the content of the attacker's Facebook accounts on the iPhone, which was seized as part of the inspection of the scene. One account was created in the name of A. and the other in a fictitious name, where he posted a video of the double murder and made a statement about the attack. The French authorities have sent a request for legal assistance regarding the information on both Facebook accounts to the US law enforcement authorities, since the service provider is under the jurisdiction of the US authorities. The latter reported that the good cause standard was met only for an account in a fictitious name due to the posting of a video of the murder, but not for a personal account. An account in a fictitious name has a direct link to the criminal act, whereas a personal account does not.[24]

[23] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. P. 43; See also [Klevtsov K.K., Vasyukov V.F., 2021: 40–41]; [Malov A.A. 2018: 56-60].

[24] Hereinafter, examples from law enforcement practice from the author's personal archive are given, with the exception of those that will be discussed separately.

Conclusion

Today, in law enforcement practice and doctrine, various approaches have been formed to determine the information that is presented in electronic form and is used in the investigation of criminal cases. Various terms are used for its designation, namely: "machine information", "computer information", "digital information", "electronic information", and in some part, and "electronic evidence". Due to the lack of legislative consolidation of these concepts and a unified point of view in theory regarding their legal nature, it is still premature to operate with them (concepts) as established categories.

As we see it, today it is worth starting from a more familiar and laconic term — "electronic information, since it is he who possesses all the necessary features, taking into account its complex and multifaceted criminal procedural essence. Under electronic information in criminal cases (in a broad sense) it is proposed to understand information transmitted by means of any physical signals (usually in electronic form), contained on the appropriate digital media, that is, in a form suitable for human perception, and which are used in the course of criminal proceedings, in particular to establish the circumstances to be proven.

At the same time, one should also take into account the classification of electronic information in the investigation of crimes, depending on: (1) stages of criminal proceedings; (2) the location of the information; (3) its content; (4) legal regulation of its obtaining; (5) its owners; (6) delivery mechanisms; (7) order of its use.

Regarding the implementation of international cooperation in the field of operational-search activities and criminal proceedings, as a rule, the following electronic information is requested: (1) basic information about the subscriber; (2) information about network transactions; and (3) content data.

References

1. Bauer F.L., Gooz G. (1990) *Computer science. Introductory course.* Moscow: Mir, 336 p. (In Russ.).

2. Balakshin V.S. (2002) *Evidence in Russian criminal procedure: concept, essence, classification.* Ekaterinburg: Ural State Law Academy, 112 p. (In Russ.).

3. Balakshin V.S. (2004) *Evidence in theory and practice of criminal procedural proof.* Ekaterinburg: Ural University, 298 p. (In Russ.).

4. Borisov A.B. (2010) Big law dictionary. Moscow: Knizhnyi mir, 848 p. (In Russ.).

5. Burnham U. (2006) *US legal system*. Moscow: Novaya justitsia, 1216 p. (In Russ.).

6. Davletov A.A. (1991) *Basics of criminal procedural knowledge.* Sverdlovsk: University, 152 p. (In Russ.).

7. Dorokhov V.Ia. (1964) The concept of evidence in Soviet criminal procedure. *Sovetskoe gosudarstvo i pravo* = Soviet State and Law, no. 9, pp. 108–117. (In Russ.).

8. Golovko L.V. (2019) Digitalization in Criminal Procedure: Local Optimization or Global Revolution? *Vestnik ekonomicheskoi bezopasnosti* = Herald of Economic Security, no. 1, pp. 22–25. (In Russ.).

9. Idowu S., Capaldi N., Zu L., Gupta A.D. (2013) Encyclopedia of Corporate Social Responsibility. Berlin: Springer: https://doi.org/10.1007/978-3-642-28036-8_100896.

10. Ivanov N.A. (2013) Digital information in criminal proceedings. *Biblioteka kriminalista* = Library of Criminalist, no. 5, pp. 93–102. (In Russ.).

11. Karas' I.Z. (1990) Economic and legal regime of information resources. *Pravo i informatika* = Law and Informatics, no. 2, pp. 40–59. (In Russ.).

12. Kasatkin A.V. (1997) Collecting and using computer information in the investigation of crimes. Candidate of Juridical Sciences Thesis. Moscow, 215 p. (In Russ.).

13. Kerr O.S. (2005) Digital Evidence and the New Criminal Procedures. *Columbia Law Review*, vol. 105, pp. 279–318.

14. Krylov V.V. (1997) *Information computer crimes*. Moscow: Norma, 285 p. (In Russ.).

15. Kushnirenko S.P. (2006) Digital information as an independent object of forensic research. *Vestnik kriminalistiki* = Herald of Criminaltics, no. 2, pp. 43–47. (In Russ.).

16. Kuvychkov S.I. (2016). Use of information presented in electronic form in proving in criminal cases. Candidate of Juridical Sciences Thesis. Nizhny Novgorod, 273 p. (In Russ.).

17. L'ianov M.M. (2020) Modern classification of virtual traces. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniia* = Siberian Criminalistics Transactions, no. 4, pp. 47–55 (In Russ.).

18. Malov A.A. (2018) Obtaining electronic evidence from foreign jurisdictions (United States as a case). *Zakonnost'* = Legality, no. 9, pp. 56–60. (In Russ.).

19. Maslov A.V., Soskova K.A. (2017) Electronic information as evidence in criminal cases. *Tsentral'nyi nauchnyi vestnik* = Central Scholar Herald, no. 11, pp. 57–59. (In Russ.).

20. Mason S. (2014) Electronic evidence: dealing with encrypted data and understanding soft-ware, logic and proof. *Journal of the Academy of European Law,* vol. 15, pp. 25–36.

21. Meshcheriakov V.A. (2004) Electronic digital objects in criminal procedure and forensic science. *Voronezhskie kriminalisticheskie chteniia* = Voronezh Criminalistics Transactions, no. 5, pp. 153–169. (In Russ.).

22. Meshcheriakov V.A. (2002) *Computer information crimes: theory and practice of investigation.* Voronezh: University, 407 p. (In Russ.).

23. Moussa A.F. (2021) Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences,* vol. 11, pp. 1–20. https://doi.org/10.1186/s41935-021-00234-6.

24. Okonenko R.I. (2016). Electronic evidence and ensuring rights of citizens to protect private life in criminal proceedings: a comparative analysis. Candidate of Juridical Sciences Thesis. Moscow, 158 p. (In Russ.).

25. Ozhegov S.I., Shvedova N. Yu. (2006) Explanatory dictionary of the Russian language. Moscow: Temp, 944 p. (In Russ.).

26. Polianskii N.N. (1946) *Evidence in foreign criminal proceedings: modern issues and trends.* Moscow: Yuridicheskoe izdatelstvo, 142 p. (in Russian);

27. Polonskii V.M. (1999) Conceptual and terminological apparatus of pedagogy. *Pedagogika* = Pedology, no. 8, pp. 16–24. (In Russ.).

28. Pitstsi U. (2019) *Litigation Without Truth: Why Our Criminal Trial System Has Become a Costly Error and What We Need to Do to Rebuild It.* Moscow: Infotropik Media, 280 p. (In Russ.).

29. Popov L.L. et al. (2010) *Information Law*. Moscow: Norma, 495 p. (In Russ.).

30. Raenko S.I. (2013) Building information society. *Nauka i sovremennost'* = Science and Modernity, no 20, pp. 189–194. (In Russ.).

31. Reshetnikova I.V. (1997) *The law of evidence in England and the USA.* Ekaterinburg: Ural State Law Academy, 237 p. (In Russ.).

32. Rothstein P.F., Raeder M.S., Crump D. (2012) Evidence in a Nutshell: State and Federal Rules. Minnesota: West Publishing Company, 816 p.

33 .Salinovskii K.V., Markelova G. Uu. (2001) Evidence-based value of electronic information in the Russian criminal process. *Rossiiskii sledovatel'* = Russian Investigator, no. 6, pp. 18–19. (In Russ.).

34. Shaidullina E.D., Shmeleva O.G. (2018) Legislative consolidation of the seizure of electronic correspondence in criminal proceedings. *Vest-*

nik Dal'nevostochnogo iuridicheskogo instituta MVD = Herald of Far Eastern Law Internal Ministry Institute, no. 2, pp. 44–49. (In Russ.).

35. Smushkin A.B. (2012) Virtual traces in forensics. Zakonnost' = Legality, no. 8, pp. 43–48 (In Russ.).

36. Sheifer S.A. (2001) *Investigation. System and procedure.* Moscow: Yurlitinform, 208 p. (In Russ.).

37. Sokolov Yu.N. (2010) *Information technologies in criminal proceedings.* Ekaterinburg: Telekommunikatsionnoe pravo, 418 p. (In Russ.).

38. Stel'makh V.Yu. (2021) The need to change the design of investigative actions aimed at obtaining information transmitted by means of communication. *Vestnik Sankt-Peterburgskogo universiteta MVD* = Herald of Peterburg University of Internal Ministry, no. 1, pp. 146–155. (In Russ.).

39. Strogovich M.S. (1986) *Soviet criminal procedure*. Moscow: Nauka, 470 p. (In Russ.).

40. Ursul A.D. (1975) *Information in modern science. Philosophical essays.* Moscow: Nauka, 287 p. (In Russ.).

41. Vasiukov V.F. (2016) Some issues of conducting investigative actions aimed at detecting, fixing and seizure of electronic messages transmitted through mobile subscriber devices of cellular communication. *Rossiiskii sledovatel'* = Russian Investigator, no. 23, pp. 15–18. (In Russ.).

42. Vasiukov V.F. (2020) Theoretical and legal aspects of crime investigation using subscriber information. Orel: Kartush, 339 p. (In Russ.).

43. Vladimirov L.E. (2000) Doctrine of criminal evidence. Tula: Avtograf. 464 p. (In Russ.).

44. Vorozhbit S.P. (2011) Electronic means of evidence in civil and arbitration proceedings. Candidate of Juridical Sciences Thesis. Saint Petersburg, 235 p. (in Russian);

45. Volevodz A.G. (2002) Countering computer crimes: legal framework for international cooperation. Moscow: Yurlitinform, 485 p. (In Russ.).

46. Vyshinskii A.Ia. (1941) *Theory of forensic evidence in Soviet law.* Moscow: Yuridicheskoe izdatelstvo, 248 p. (In Russ.).

47. Walker C. (2001) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. *Crime Prevention and Community Safety,* vol. 3, pp. 87–88.

48. Zaitsev O.A. (2019) Using electronic information as evidence in a criminal case: a comparative analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = Journal of Foreign Legislation and Comparative Law, no. 4, pp. 42–57. (In Russ.).

49. Zazulin A.I. (2018) Legal and methodological foundations for using digital information as proof in a criminal case. Candidate of Juridical Sciences Thesis. Ekaterinburg, 251 p. (In Russ.).

50. Zhdanko A.V. (2013) *Introduction to General Historiology.* Saint Petersburg: Aleteiya, 277 p. (In Russ.).

51. Zigura N.A. (2010) Computer Information as a type of evidence in criminal procedure in Russia. Candidate of Juridical Sciences Thesis. Chelyabinsk, 234 p. (In Russ.).

52. Zigura N.A., Kudriavtseva A.V. (2011) *Computer information as a type of evidence in the criminal process of Russia.* Moscow: Yurlitinform, 176 p. (In Russ.).

Information about the author:

K.K. Klevtsov — Candidate of Science (Law), Associate Professor.

The article was submitted 10.09.2021; approved after reviewing 22.11.2021; accepted for publication 29.11.2021.

Legal Issues in the Digital Age. 2021. Vol. 2, no. 4.

Comment

Comment
UDC: 347
DOI: 10.17323/2713-2749.2021.4.130.142

Judicial Protection of Intellectual Property Rights in a Digital Economy: Is There a Need for Change?

Natalya Vladimirovna Buzova,[1]

Marina Maksimovna Karelina[2]

[1,2] Russian State University of Justice, Moscow, Russia.

[1] nbuzova@yandex.ru. ORCID: 0000-0003-2268-0345

[2] ip_laboratory@mail.ru. ORCID 0000-0002-8982-3710

Abstract

The paper looks at improving the judicial system in Russia facing the rapid technological change of modern society in which new relationships are largely associated with different areas of intellectual property. Today biotechnology, digital rights, computer programs and scientific research materials have become widely used in civil circulation and their intellectual property rights should be effectively protected. The paper discusses different issues of protecting intellectual rights provided for by the Civil Code of the Russian Federation, aimed at both suppressing and preventing their infringement, and assesses the statistical indicators of the courts. The practice of the Intellectual Property Rights Court and the Moscow City Court shows that specialization yields positive results. The selection of judges, their professional development including their distinctive competencies in addition to legal ones, also help to find effective ways of resolving intellectual property disputes. With the protection of intellectual property rights being of great concern not only in Russia, but also in most developed countries of the world, their experience has also been thoroughly analyzed. The paper suggests a possible way of improving the judicial system under the current circumstances. Certain changes in the judicial system and the creation of additional specialized intellectual property courts could

help to ensure an affordable, legitimate and effective mechanism for resolving disputes related to the violation of intellectual property rights.

Keywords

intellectual property, intellectual rights, exclusive right, court, judicial protection, judicial system

For citation: Buzova N.V., Karelina M.M. Judicial Protection of Intellectual Property Rights in a Digital Economy: Is There a Need for Change? *Legal Issues in the Digital Age.* 2021, vol. 2, no. 4, pp. 130–142. DOI: 10.17323/2713-2749.2021.4.130.142.

Intellectual property in modern societies is a key driver of its economic, social and cultural development. The introduction of the new technologies creates complex networks of social relations. There are intense discussions underway about legal regulation of relations in the field of artificial intelligence; experimental legal acts are being adopted[1]. The transition from the traditional civil law relations, pivoted on the notions of a material object and obligation to the novel and much more complex relations based on such ideas as human impact on complex biological objects [Vasiliev S.A., et al, 2017: 71], digital technologies, etc., generates a previously unknown type of relations.

What is important is that these new relations, in one way or another, involve the use of intellectual property (IP). For instance, in telecommunication networks, items protected by copyright and related rights account for more than 80% of the content. Software programs for electronic computing machines are the main instrument used across the entire spectrum of disciplines by researchers today [Schwab K., 2018: 31–46]. So, ensuring effective protection for copyrighted items is a most important factor for the functioning of modern states.

[1] See: Federal law No. 123-FZ (April 24, 2020) "On Conducting the Experiment to Establish a Special Regulatory Mechanism in order to Create Necessary Conditions for Developing and Introducing Artificial Intelligence Technologies in Moscow, a Region of the Russian Federation and a City with Federal Status, and on Introducing Amendments to Articles 6 and 10 of Federal law 'On Personal Data'" [O provedenii eksperimenta po ustanovleniyu spetsial'nogo regulirovaniya v tselyakh sozdaniya neobkhodimykh usloviy dlya razrabotki i vnedreniya tekhnologiy iskusstvennogo intellekta v sub"ekte Rossiyskoy Federatsii — gorode federal'nogo znacheniya Moskve i vnesenii izmeneniy v stat'i 6 i 10 Federal'nogo zakona «O personal'nykh dannykh»]. Available at: http://www.pravo.gov.ru (accessed: 24.04.2020)

Justice systems have to respond to the challenges brought about by the 4th technological revolution, and this is a challenge that any developed nation, no matter what its legal system is, has to face.

The Agreement on Trade-Related Aspects of Intellectual Property Rights[2] (hereinafter referred to as TRIPS) obligates its signatories to have "enforcement… available under their law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement." At the same time, the TRIPS Agreement "does not create any obligation to put in place a judicial system for the enforcement of intellectual property rights distinct from that for the enforcement of law in general" (Art.41(1 and 5)).

However, although the international agreements do not obligate states to set up specialized courts for adjudicating disputes concerning intellectual property rights (IPR), a general trend to create such courts is on the rise in the vast majority of economically developed countries.

As the weight of IP in national economies grows, there is an increasingly stronger focus on the effectiveness of protection of copyright and related rights. There are certain items of intellectual property which cannot be protected by means of self-defense, such as, for instance, technological safeguards. Besides, due to their very nature most of copyrighted items and identifications (except manufacturing secrets) are intended to raise public awareness and promote goods, works and services on the market — in other words, their open use is the norm. In view of this, there is a growing demand for judicial protection of infringed or contested IPR, which rights, pursuant to Art.1226 of the Civil Code of the RF, apply to protected identifications and results of intellectual activity.

The Russian legislation provides for a wide range of legal remedies in the field of IPR, intended to stop, as well as prevent, infringements thereof. Infringements of IPR in the Russian Federation are punishable under civil, criminal and administrative law. Depending on the character, degree of public danger, and consequences of an infringement, IP disputes can be treated as public or private law cases.

According to the court statistics[3], the amount of court cases involving IP-related alleged criminal and administrative offenses has been declin-

[2] Agreement on Trade-Related Aspects of Intellectual Property Rights [Soglashenie po torgovym aspektam prav intellektual'noy sobstvennosti] (Marrakesh, April 15, 1994). A Russian-language version // SPS Garant.

[3] Court Statistics. The Department of Courts under the aegis of the Supreme Court of the Russian Federation. Available at: URL: http://www.cdep.ru. (accessed: 16.11.2020)

ing in recent years. While in 2009 the courts heard 12,511 cases of administrative offenses covered by Art.7.12 of the Code of Administrative Offenses and involving infringements of copyright and related rights, inventors' rights, and patent rights, in 2020 the courts heard 706 such cases; whereas in 2009 1,631 people received criminal convictions solely on account of infringements of IP and related rights, pursuant to Art.146(2) of the RF's Criminal Code, in 2020, only 155 people in the RF received criminal convictions in all proceedings related to infringements of IPR, including patents and trademarks (Art. 146, 147, 180 of the RF's Criminal Code). The number of IP-related civil cases, meanwhile, is growing exponentially. According to the court statistics, the overall amount of civil cases handled both by general jurisdiction courts and arbitrazh courts have grown from 4,056 (in 2009) to 28,350 (in 2020). Rights holders seek not so much to punish the violators as put an end to their unlawful doings and receive a compensation for the infringements of IP rights. This article, therefore, is focused on civil disputes over breached or contested IP rights.

Some international agreements — for instance, Art.33 of the Berne Convention for the Protection of Literary and Artistic Works (Berne, Sept. 9, 1886, hereinafter referred to as the Berne Convention), Art.28 of the Paris Convention for the Protection of Industrial Property (Paris, March 20, 1883), Art. 30 of the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome, Oct. 26, 1961) provide for an option of applying to an international court of law. This option, however, is reserved not for economic entities whose exclusive rights, covered by relevant international agreements, to copyrighted items and identifications have been breached but for member states who recognize such a court and only in relation to disputes over interpretation or application of a relevant convention, if these disputes cannot be settled by negotiation. There is no information available about any state applying to an international court during the period when the multi-lateral IP agreements providing for this option have been in place. The foundational multi-lateral international IP agreements — for instance, Art.5 of the Berne Convention — assert the primacy of national protection regimes: for instance, as per Art.5 of the Berne Convention, "the extent of protection [of IPR], as well as the means of redress afforded to the author to protect his rights, shall be governed exclusively by the laws of the country where protection is claimed," that is the rights holder whose rights has been breached applies to the court of the country where the infringement took place and not to an international court.

The World Intellectual Property Organization (WIPO) runs an Arbitration and Mediation Center[4], whose mission is to facilitate settlements of IP- and technology-related commercial disputes between private persons. This Center, however, is focused on mediation and the effectiveness of its decisions depends on the parties' readiness to compromise, find mutually acceptable tradeoffs and continue their cooperation in the area of IP in the future.

The Eurasian economic space now has a new international court. Pursuant to the Treaty on the Eurasian Economic Union (signed on May 29, 2014, in Astana)[5] a Court of the EAEU was established. The court's remit, established in Art. 39 of the Statute of the Court of the EAEU[6], is limited to adjudicating disputes over the realization of the Treaty on the EAEU, international agreements within the EAEU, and decisions of the EAEU's organs, to wit, the Eurasian Economic Commission (EEC). An economic entity may apply to the Court of the EAEU to contest an action (or inaction) of the EEC which has a direct bearing on the entity's rights and lawful interests, if this action (inaction) has caused a breach of rights granted under international agreements within the EAEU, or to contest a decision of the EEC on the grounds that it allegedly breaches the entity's rights and does not conform with international agreements within the EAEU. In other words, the new international court does not consider disputes over infringements of IPR involving economic entities from the EAEU's member states.

In the RF cases involving the protection of infringed or contested IPR are heard by the courts of general jurisdiction or arbitrazh courts, depending on the subject matter jurisdiction.

The Arbitrazh Court for Intellectual Property Rights occupies a special place. The legal groundwork for the establishment and operation of this Court was laid in federal constitutional law No. 4-FKZ (Dec.6, 2011)[7],

[4] For more details, see WIPO Arbitration and Mediation Center. Available at: https://www.wipo.int/amc/en/center/background.html. (accessed: 16.11.2020)

[5] Available at: www.pravo.gov.ru. (accessed: 16.11.2020)

[6] The Statute of the Court of the Eurasian Economic Union. Annex 2 to the Treaty on the Eurasian Economic Union Signed on May 29, 2014. Available at: URL: https://courteurasian.org/upload/iblock/b30/2 (accessed: 16.11.2020)

[7] Federal Law No. 4-FKZ Dec.6, 2011 "On Introducing Amendments to Federal Constitutional Law 'On the Court System of the Russian Federation' and federal constitutional law 'On Arbitration Courts in the Russian Federation' On Occasion of the Establishment of the Court for Intellectual Property Rights in the System of Arbitration Courts" [O vnesenii izmeneniy v Federal'nyy konstitutsionnyy zakon «O sudebnoy sisteme Rossiyskoy Federatsii» i Federal'nyy konstitutsionnyy zakon «Ob arbitrazhnykh sudakh v Rossiyskoy Federatsii" v svyazi s sozdaniem v sisteme arbitrazhnykh sudov Suda po intellektual'nym pravam]. Compendium of Laws of the Russian Federation. 2011. No. 50. Art. 7334.

which introduced amendments to federal constitutional law No. 1-FKZ (Apr.28, 1995) "On Arbitrazh Courts in the Russian Federation" and federal constitutional law No. 1-FKZ (Dec.31, 1996) "On the Court System of the Russian Federation."

The powers of the IP Court are set out in chapter IV.1 of federal constitutional law No. 1-FKZ (Apr.28, 1995) "On Arbitration Courts in the Russian Federation" (with amendments) and its jurisdiction mostly covers industrial intellectual property; this Court is a specialized arbitrazh court which hears, in its capacity as the first-instance court and the court of cassation, cases concerning protection of IPR, as well as challenges of bylaws issued by federal executive bodies in relation to patent rights, breeders' rights, rights to topographies of integrated circuits, manufacturing secrets (know-how), identifications of corporate entities, goods, works, services and enterprises, and rights to use copyrighted items in technology transfers [9. C. 80–84].

Other matters within the Court's jurisdiction include disputes over the grant and termination of legal protection for results of intellectual activity and items equated to them such as identifications of corporate entities, goods, works, services and enterprises (except items protected by copyright and related rights, topographies of integrated circuits), as well as cases involving identification of patent holders; cases involving invalidation of patents for inventions, utility models and industrial designs or breeding patents; cases involving invalidation of decisions to grant a protection title for trademarks and appellations of origin and decisions to grant exclusive rights to such appellations, unless a federal law provides for different invalidation procedures; cases involving invalidation of decisions about early termination of a protection title for trademarks on account of their disuse.

The IP Court is authorized to resolve disputes challenging special bylaws, decisions and actions (inaction) of a federal executive organ responsible for IP and a federal executive organ responsible for breeding, and officers of such organs, as well as organs authorized by the RF's government to review applications for patents for secret inventions. [Translator's note: special bylaws — *nenormativnye pravovye akty:* acts targeting "a small, identifiable group for treatment that does not apply to all the members of a given class" (from a Wikipedia article on special legislation).] The Court hears cases involving challenges of the federal anti-monopoly organ's decisions to recognize as unfair competition actions related to acquisition of an exclusive right to identifications of corporate entities, goods, works, services, and enterprises.

Beginning from 2016 the IP Court has been adjudicating disputes over normative acts, issued by federal executive organs, which contain explanations of legal norms and concern patent rights and breeders' rights, rights to topographies of integrated circuits, rights to manufacturing secrets (know-how), rights to identifications of corporate entities, goods, works, and enterprises, and rights to use copyrighted items in technology transfers (para 1.1 was introduced by federal constitutional law No. 2-FKZ of February15, 2016).

Importantly, the mentioned types of disputes are considered by the IPR Court irrespective of the identity of the parties to the dispute, be it organizations, sole traders or private persons. In other words, the Court has a wider jurisdiction in relation to private persons than some arbitrazh courts.

But as for copyrighted items, the IPR Court hears them only in its capacity as the court of cassation.

Court statistics for IP-related cases heard by different courts of the RF in 2020 is provided in Tables 1-3.

Table 1

Statistics on cases heard by the RF's IPR Court in 2020

Number of cases	Challenges of normative legal acts	On granting or terminating a title of protection	On early termination of a title of protection for a trademark due to its disuse	Total, including other categories
Heard	1	894	341	937
Requests granted	0	307	153	311

Table 2

Statistics on IPR-related civil cases at the arbitrazh courts in the RF in 2020

Number of cases	Trademark infringements	Infringements of copyright and related rights	Patent infringement	Total, including other categories
Considered	11,549	5,528	95	25,836
Requests granted	9,490	4,466	45	20,898

Table 3

Statistics on IP civil cases heard by the courts of general jurisdiction in the RF in 2020[8]

Number of cases	Infringements of copyright and related rights	Patent infringements	Protection of copyright and/or related rights on the Internet (Art.26(3) of the RF's Code of Civil Procedure)	Total
Considered	645	36	1,158	2,219
Requests granted	379	32	1,089	1,707

The court statistics shows that the arbitrazh courts account for a major portion (89%) of IPR civil cases in the RF. This is because many disputes arise from business and other similar transactions and from instances of unlawful trade in goods which breach exclusive rights to copyrighted items and identifications. Another thing to keep in mind is that the arbitrazh courts are the forum for disputes over identifications[9] and protection of IPR the parties to which include collecting societies.[10] Besides, certain categories of cases — for instance, disputes over the authorship of inventions, utility models, industrial designs, breeding patents — are the purview of the IPR Court, which is a part of the system of arbitrazh courts.

The prospects of creating a specialized court for intellectual property — in particular, a patent court — were discussed yet in the Soviet Union, up until 1992–1993, when the RF adopted [Yeremenko V.I., 2012: 22] the laws

[8] Report on First-Instance Hearings of Civil and Administrative Cases in the Courts of General Jurisdiction in 2018. The Department of Courts under the aegis of the Supreme Court of the Russian Federation. Available at: URL: http://www.cdep.ru/index.php?id=79&item=4891 (accessed: 16.11.2020)

[9] There can be exceptions such as disputes over appellations of origin of goods involving private persons (rather than corporate entities / sole traders): for instance, an artisan or a non-Russian citizen who holds an exclusive right to use an appellation of origin in the RF. Such disputes are to be heard by a court of general jurisdiction.

[10] For more detailed information about the handling of the cases by the courts of general jurisdiction and arbitrazh courts, see the explanation of the Supreme Court of the RF in para 3 of resolution No. 10 (Apr.23, 2019) of the Plenum of the Supreme Court of the RF "On Application of Part IV of the Civil Code of the Russian Federation."

on trademarks, copyright, and patents; however, the idea to set up a specialized court was not realized at that time. Instead, the RF's lawmakers authorized a quasi-judicial form of adjudication on matters concerning the issuance of protection titles and the grant of exclusive rights to certain items of intellectual property: the relevant provisions were contained in law on patents No. 3517-I (Sept.23, 1992) and law of the RF No. 3520-I (Sept.23, 1992) "On Trademarks, Service Marks, and Appellations of Places of Origin of Goods."

The growing numbers of cases involving contested IPR related to business transactions that the arbitrazh court had to handle (for instance, 3,482 cases in 2009 and 9,237 in 2013) was one of the factors spurring the establishment of a specialized IPR court in the RF. In order to reduce the length of proceedings and enhance their effectiveness in IPR cases [Korneev V.A. 2011: 2], the IPR Court was established and started operating on July 3, 2013.

Speaking about judicial protection of copyright and related rights, one should not forget to highlight the Moscow City Court — it handles, inter alia, in its capacity as the first-instance court, civil cases which concern protection of copyright and related rights, except rights to photographs and items that were produced by means similar to photography and published in information and telecommunication networks, including the Internet, and in which this court has granted injunctive relief.

The changes in technologies and in communication and data storage devices used to reproduce works and copyrighted items call for new approaches to the protection of copyright and related rights. While at the time when the RF adopted its law No. 5351-I (July 9, 1993) "On Copyright and Related Rights" (hereinafter referred to as the Copyright Law) works and copyrighted items were reproduced with the use of VHS tapes, cassettes and disc records, the early 2000s saw the advent of optical storage devices for laser-beam systems, and from 2010 on, users of items protected by copyright and related rights, at first gradually and then en masse, have been using the information and telecommunication networks, including the Internet.

Under Art. 48 of the Copyright Law, phonorecords and copies of works whose manufacturing or distribution involved an infringement of copyright and related rights were deemed to be counterfeits. While the Copyright Law was in effect, the cassettes and discs were the foremost storage devices for works and items protected by related rights, so the focus was on police investigations aimed at discovering businesses manufacturing and selling counterfeit goods; the effective legal remedies, accordingly, consisted in shutting down facilities where counterfeit goods were manufac-

tured and sold and in confiscating and destroying the equipment, materials and data storage devices used by infringers of copyright and related rights. Later the mentioned remedies against infringements of copyright and related rights became somewhat obsolete since the Internet became the space where the majority of infringements take place.

The first step taken to put an end to unlawful use of cinematic, televised and other audiovisual works was the adoption of Federal Law No. 187-FZ (July 2, 2013) "On Introducing Amendments to Certain Legal Acts of the RF With Respect To the Protection of Intellectual Property Rights in the Information and Telecommunication Networks," often referred to as "the anti-piracy law," which, beginning from Aug.1, 2013, authorized courts to issue injunctions to protect exclusive rights to audiovisual works on the Internet (Art.144.1 of the RF's Code of Civil Procedure). The law prescribes a procedure whereby courts can restrict access to films unlawfully posted on (or, to put it more accurately, unlawfully brought to general notice via) the Internet or remove such works pursuant to a rights holder's complaint. Granting preliminary injunctive relief to protect copyright and related rights on the Internet is a responsibility of the Moscow City Court. The positive effect of the "anti-piracy law" has demonstrated the wisdom of the decision to expand the available remedies. The next step to put an end to unlawful use of copyrighted items on the Internet was to expand the "judicial mechanism" to apply to all objects of copyright and related rights which can be used on the Internet, except photographs (Federal Law No. 364-FZ (Nov.24, 2014) "On Introducing Amendments to the Federal Law 'On Information, Information Technologies, and Protection of Information' and to the Code of Civil Procedure of the Russian Federation"). The law also authorizes courts to block access to those sites in the Internet on which copyrighted items were repeatedly unlawfully posted.

Despite the obvious positive effect from the conferral of additional powers on the Moscow City Court as provided by Art. 26 (3) of the RF's Code of Civil Procedure, one cannot fail to notice an increase in the court's caseload: from 446 cases in 2016 to 1,158 in 2020.

The RF is making a transition to digital economy — an environment which reduces the lengths of time needed to spread information, makes it possible to process large reams of data, and introduces new technologies — and this transition opens up new opportunities for using copyrighted items in digital formats. Given that copyrighted items and identifications are immaterial, a fair and comprehensive consideration of IPR cases, especially cases involving digital items, requires not only the knowledge of law but

also expertise in other fields, including technical. At the same time, a weak protection of IPR in business matters can have a negative impact on the national economy's attractiveness to investors and competitiveness. In view of this, it would seem advisable to continue the search for additional guarantees of fair justice — the system that would enable judges to quickly and effectively resolve the complex disputes in a continuously changing technological environment.

As has been noted earlier, the global trend is to have specialized courts adjudicate on IPR dispues, although different countries handle these matters differently, depending on the specifics of local legislative frameworks and economic and social development [de Werra J., 2016: 17]. The crucial question in the debate about the need for specialized IPR courts is enhancing the efficiency of the application of law in the area of IP. An analysis of the case law of the IPR Court and the Moscow City Court shows that the specialization brings good results although this is only the first stage. Creating a system that would produce a consistent case law without separation by the subject matter (an IP court) or by the parties and procedure (Moscow City Court) [7] would appreciably strengthen the effectiveness of protection of IPR in a rapidly changing technological landscape in the RF in the 21st century. According to different estimates, IP can account for 25–30% of the GDP and this share has a tendency to grow.

Developing a system of specialized IPR courts can probably promote the growth of effectiveness of the application of IPR law. So, what are the issues that need to be addressed when considering the prospect of creating of a single special court for IPR disputes?

It should be kept in mind that the mission of specialized IPR courts is to ensure an accessible, equitable and efficient mechanism for resolving disputes involving infringements of copyright and related rights — this system requires highly competent judges possessing, in addition to other things, a good knowledge of high technology.

The question of training and selecting judges is therefore one of the most important ones: it is essential for such judges to be competent in other fields besides law in general, and they should also be afforded opportunities of ongoing learning, which would keep them abreast of quickly occurring changes in IP law and national and international case law in this area.

The subject matter jurisdiction of these courts needs to be defined — for instance, in some jurisdictions IPR courts handle not only IP disputes but anti-monopoly cases as well. Procedures for appealing these courts' decisions should be in place as well.

The current legislation, as it seems, allows for the establishment of specialized courts within the system of courts of general jurisdiction: this follows from Art.4 of federal constitutional law No. 1-FKZ (Dec.31, 1996) "On the Court System of the Russian Federation" (amended version) [Orlova V.V. et al. 2007: 67].

For instance, the RF could establish specialized courts to resolve cases, in their capacity as the first-instance court, involving IPR and digital technologies. Such courts could be arranged along the same regional lines as the system of general jurisdiction courts of appeal and courts of cassation. Such specialized courts could each cover a group of regions.

Speaking about international experience, one should take notice of the district courts in Belgium specializing in IP disputes, as well as the High Courts of Korea, set up in Seoul, Busan, Daegu, Daejon, and Gwangju[Adjudicating Intellectual Property Disputes:2016]].

The IPR Court could become the forum for appeals against rulings of these courts, whereas the IP and digital technologies panel of the RF's Supreme Court could function as the court of cassation.

References

1. Adjudicating Intellectual Property Disputes. An ICC report on specialised IP jurisdictions worldwide. International Chamber of Commerce (2016). Available at: URL: http://www.iccbooks.ru/upload/iblock/402/402fae44939769a4b61225ae6bea8cbe.pdf.

2. Court for Intellectual Property Rights (2013). The History of Its Creation and the Prospects of Its Development. Moscow: INITS "PATENT," 2013. 183 p. (In Russ.).

3. *The Court for Intellectual Property Rights and Its Place Among the Public Authorities in the Russian Federation* (2015). Eds. Bliznets I.A., Novoselov L.A. Moscow: Prospect, 120 p. (In Russ.).

4. International conventions on Copyright Law. Comment. Gavrilov E.P. (ed.). Moscow: Progress. 1982. 243 p. (In Russ.).

5. Korneev V.A. (2011) What the Court for Intellectual Property Rights Will Be Like? *Patenty i litsenzii* = Patents and Licensing, no. 1, pp. 2–6. (In Russ.).

6. Lubimova E.V. (2019) Jurisdiction of the Court on Intellectual Rights. *Ex jure*, no. 3, pp. 29–42. (In Russ.).

7. Novoselova L.A., Sergo A.G. (2017) On perspectives of using mediation for regulation of conflicts on intellectual property. *University named after O.E. Kutafin Bulletin,* no. 6, pp.17–24. (In Russ.).

8. Orlova V.V. et al. (2007) What Type of Patent Court Russia Should Have? Moscow: Patent, 77 p.

9. Pirozhkov A.V. (2014) How the Courts Apply Federal Law No. 187-FZ (July 2, 2013) "On Introducing Amendments to Certain Legal Acts of the Russian Federation Concerning Protection of Intellectual Property Rights in the Information and Telecommunication Networks". *Rossiyskoe pravosudie* = Russian Justice, no. 6 (98), pp. 62–77. (In Russ.).

10. Popova S.S. (2013) Problems of the formation of the Court on Intellectual Rights in Russia. *Imuzhestvennie otnoshenia v Rossiiskoi Federatii* = Property Relations in Russian Federation, no. 6(141), pp. 96–106. (In Russ.).

11. Schwab K. (2018) *The Fourth Industrial Revolution*. Moscow: EKSMO, 208 p. (In Russ.).

12. Sidorenko A.I. (2019) Court protection of intellectual rights in the digital era. *Zhurnal rossiiskogo prava* = Journal of Russian Law, no. 8, pp. 136–147. (In Russ.).

13. Vasiliev S.A., Osavelyuk A.M., Burtsev, A.K., Suvorov G.N., Sarmanaev S.Kh., Shirokov A.Yu. (2019) Problems of Legal Regulation of Genome Diagnostics and Gene Editing in Humans in the Russian Federation. *Lex Russica*, no. 6, pp. 71–79. (In Russ.).

14. de Werra J. (2916) Specialized Intellectual Property Court — Issues and Challenges. Second Issue, Global Perspectives for the Intellectual Property System, no. 2. Available at: URL: https://www.ictsd.org/sites/default/files/research/Specialised%20Intellectual%20Property%20Courts%20-%20Issues%20and%20Challenges_0.pdf.

15. Yeremenko V.I. (2012) On Establishing a Court for Intellectual Property Rights in the Russian Federation. *Zakonodatel'stvo i ekonomika* = Legislation and Economy, 2012, no. 8, pp. 9–22. (In Russ.).

Information about the authors:

N.V. Buzova — Candidate of Sciences (Law), Leading Scholar.

M.M. Karelina — Head of the research project.

The article was submitted 22.09.2021; approved after reviewing 12.11.2021; accepted for publication 26.11.2021.

During preparing of the current issue M.M. Karelina passed away after Covid-19. We knew her as a wonderful human person full of life and plans.

Articles

Comment

Review

Book Review

Articles

Review

Articles

Comment

23rd YASIN (APRIL) INTERNATIONAL ACADEMIC CONFERENCE ON ECONOMIC AND SOCIAL DEVELOPMENT

HSE University is pleased to announce a call for proposals to take part in the 23rd International Academic Conference on Economic and Social Development. Following the decisionof the University's Academic Council, starting from 2022, the Conference will be called the YasinConference in honour of Evgeny Yasin, the Honorary Academic Supervisor of HSE University, who launched the Conference, which has become a major annual academic event in Russia in thesocial sciences (as we know it now).

The key events under the 23rd Yasin (April) International Academic Conference on Economic and Social Development (23rd Yasin Conference) will take place in Moscow from April4 until April 8, 2022.

At sections under the 23rd Yasin Conference, reports will be presented and discussed on the results of recent academic research, selected through reviews of proposals (the requirements for which can be found below). In addition, the Conference will include expert discussions on themost pressing problems in regards to economic and social policies, involving leading Russian andglobal specialists and public officials, as well as honorary reports presented by academics from allover the world and various associated events. The Conference's events will be held in Russian orEnglish; certain discussions will be bilingual and supported by simultaneous translation.

We invite you to register as a listener of the XXIIIYIAC. Detailed information is available at https://conf.hse.ru/2022/

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 *Р.С. Рааб*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*