ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

2/2021

Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

2/2021

ISSUED QUARTERLY

Articles

Review

Publisher
National Research
University Higher School
of Economics

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

Law and Digital Transformation[1]

Yuri Tikhomirov

Public Law Research Center, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Doctor of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: tikhomirov@izak.ru

Nikolai Kichigin

Leading Researcher, Institute of Legislation and Comparative Law Under the Government of the Russian Federation, Candidate of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: ecology@izak.ru

Fatima Tsomartova

Senior Researcher, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Candidate of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: social3@izak.ru

Sayana Balkhayeva

Leading research fellow, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Candidate of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: foreign1@izak.ru

Abstract

The coexistence of digitization and law fuels their mutual influence and calls for scholarly inquiry into their mutual impacts and the effects thereof. Technization of society has contributed to society's development, and the objectives and vectors of this process have been in many ways informed by public and other social institutions, including law. Like before, digitization at its current stage combines social and technological mechanisms of managing societal processes, ingrained into the wide socio-economic context and connected with the implementation of the nation's strategic objectives. Similar phenomena and processes have a strong impact beyond Russia's borders as well. All this poses challenges for law. The article is an attempt to analyze legal challenges of digitization applying the method of comprehensive, intersectional and systemic analysis, which breaks down the excessive compartmentalization of sector-specific legal sciences and takes into account the relationship between national and international law, as well as advances in other social sciences. The new digital technologies transform law's functionality, and this, firstly, is reflected in the dynamically developing sector-specific legislation,

[1] The original article was published in "Law. Journal of the Higher School of Economics" no 2, 2021.

and secondly, adds a distinctive dimension to the new laws and regulations of general character that create the basis for digitization. Digitization transforms the way subjects of law operate and the volumes of legal relations between them; generates new forms of administrative decision-making and of liability for non-implementation of these decisions; problematizes the subject area of the legal nature of technical (electronic) legal acts and the place they occupy in the legislative and regulatory framework; highlights the issue of the potential and limitations of automation of law. The study leads the researchers to conclude that in the age of digital transformation of economy, social sphere and public administration, law steadily continues to function as the regulator of socio-economic and other processes in society, ensuring both stability and the necessary transformational activities of individuals and public institutions.

Keywords

digitization, national law, international law, sectoral legislation, digital law, technical (electronic) legal acts, digital rights, automation of law, subject of law, liability.

For citation: Tikhomirov Yu.A., Kichigin N.A., Tsomartova F.V., Balkhayeva S.B. (2021) Law and Digital Transformation. *Legal Issues in the Digital Age,* no 2, pp. 3– 20.

DOI: 10.17323/2713-2749.2021.2.3.20

Introduction

Does law change in the age of digital transformation? This question is very important both theoretically and practically. The introduction of new digital technologies in different spheres of public life creates an impression that social contacts are quick in the making and transparent for the public and decisions are made directly, through an open dialog. This commonplace perception has deep roots, although it needs to be examined through a scholarly lens.

Law is a neat system of binding laws and rules regulating relations within society, individuals' conduct, and organizations' activities. By now Russia has a fairly well developed body of laws, which is being quickly updated due to the pandemic, the difficulties in international relations and, finally, the amendments to the Russian Constitution, requiring dynamic adaptation of the legislation [Khabrieva T.Y., Klishas A.A., 2021]; [Khabrieva T.Y., 2016].

Now we have two phenomena at play: classical, traditional, regularly updated law — and digitization, which reflects the new character and the new language used by individuals and organizations interacting with each other. How do these two phenomena link up and influence one another,

which one is more important, and can it be that one phenomenon is edging out another? Any simple answer to these questions is certain to be incorrect because while law strongly influences the process of digitization, digitization, in turn, influences legislative regulation and its forms, as well as individuals' legal awareness.

1. Legal problems of digitization

Thinkers of the past spent a lot of effort trying to solve the riddles of scientific progress. They believed that in the society of the future there would be different regulators. Friedrich Engels in his work "Anti-Dühring" supposed that in the future "the government of persons [would be] replaced by the administration of things, and by the conduct of processes of production." But the government of persons does not die out: persons themselves govern these processes, as well as their own mutual transactions. Our country in the 1970s was developing a national automated system of economic governance. So the subject discussed here did not appear out of nowhere — it has an eventful history. People have been thinking about how to use scholar and technological advances for solving social, economic and other problems.

The last few years have seen the publication of works addressing specifically the issue of digitization from a legal perspective: their authors propose a legal concept of robotization, review issues related to breaches of laws and regulations in the new digital settings, describe the specifics and prospects of legislative regulation of data exchanges in public administration [Talapina E.V., Yuzhakov V.N. et al., 2020]; identify environmental imperatives in laws and life [Bogolyubov S.A., 2020], which also need a robust informational support; research transformations of the institutions of budget law in the age of digital revolution [Artyukhin R.Ye., Povetkina N.A., 2021], etc. These studies show that some academic groundwork in the field has been done already, the basis is already in place and needs to be built upon.

At the same time, as law and scientific progress continue to interact, many new and interesting issues come up. The first issue in need of comment is overlaps between legal regulation and digitization. Digitization "sweeps into" various spheres, sometimes causing harm to people, and sometimes making their life easier and facilitating organizations' activities.

In the matters of public administration, digitization has a significant impact on public agencies' functionality so that some functions die off while others become substituted. In particular, the colossal flow of accounting and audit documents is substituted with more useful and efficient analyti-

cal and forecasting tools. The introduction of the new methods of data exchange allows to expand the informational foundation for administrative decisions and actions, significantly facilitating the task of public administration.

In the area of economy, robots are being introduced in great numbers in manufacturing and construction, successfully managing a great variety of manufacturing and technological tasks. The innovations in the service sector and social services are especially striking. Many services are gradually converted to electronic formats — individuals can use online portals to solve problems related to their pension, labor, housing and other social rights. In educational, academic and cultural spheres, a lot of things are going online as well. Thus, during the pandemic classes little by little went online. In such areas as ecology, environmental protection, the fight against climate change, and the protection of forests and other natural resources, new monitoring technologies are likewise very important: digitization does good.

The second issue concerns the changes in law in the age of universal introduction of modern digital technologies. The object of legal regulation is transformed while the social role of law in streamlining social interactions remains the same. The functional impact of law, meanwhile, changes, which is reflected, first of all, in the dynamically developing sectoral legislation: civil [Sinitsyn S.A., 2020: 73–171], labor, ecological, administrative, educational, health care law, etc.

In particular, provisions concerning digital rights are added to Russia's Civil Code while amendments to Russia's Labor Code reflect the new modes of employment. Overall, one should keep watching sectoral legislation: although quite well developed, it needs modernization to ensure that individuals and organizations/businesses can easily interact with each other using electronic technologies.

In addition to sectoral legislation, one would want to point to the recent legal acts of general nature creating a basis for digitization. The Strategy for Developing an Information Society in the Russian Federation for 2017-2030 was created yet in 2017;[2] impressive state program Information So-

[2] Decree of the President of the Russian Federation No. 203 May 9, 2017 "On The Strategy of Development of an Information Society in the Russian Federation for 2017-2030" [O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody]. In: Compendium of Laws of the Russian Federation [Sobranie zakonodatel'stva Rossiyskoy Federatsii]. 2017. No 20. Art. 2901.

ciety is afoot;[3] the National Strategy for Developing Artificial Intelligence for the Period until 2030 was adopted;[4] a special legislation about digital financial assets is in place.[5] All this bodes well for the introduction of digital technologies into everyday use. The process is not easy because each sphere has a large stream of regulatory paperwork, including technical standards. Because these regulatory documents are very important, the modernization thereof is of the highest priority. Changes to some regulatory instruments, however, are introduced very quickly and without any concern for other related instruments, while updates to some other regulations are obviously slower to come about, so systematic updating is the objective to pursue.

The adoption of laws and other legislative instruments concerning technical norms has been a conspicuous tendency as of late. In different countries of the world law has made a significant progress in this direction: South Korea adopted the Intelligent Robots Development and Distribution Promotion Act (2008); the EU has the Civil Law Rules on Robotics (2017);[6] the Republic of Belarus on July 17, 2018, adopted a Law on Laws and Other Legislative Instruments (No. 130-3), introducing the concept of technical laws and regulations. Russian legal scholars, too, are increasingly more preoccupied with such issues as legal validity of new documents, new legal acts called technical or electronic. But the main problem is to find a place for this new type of solutions, new type of legal acts in the legislative and regulatory framework.

There are changes underway in the relationship between individuals and new technical devices, which are reflected in the status of both governmental agencies and their individual employees. Whereas previously each

[3] Order of the Government of the Russian Federation No. 313 April 15, 2014 "On Approving the State Program of the Russian Federation 'Information Society'" [Ob utverzhdenii gosudarstvennoy programmy Rossiyskoy Federatsii "Informatsionnoe obshchestvo"]. Ibid. 2014. No. 18. Art. 2159.

[4] Decree of the President of the Russian Federation No. 490 October 10, 2019 "On Developing Artificial Intelligence in the Russian Federation" [O razvitii iskusstvennogo intellekta v Rossiyskoy Federatsii]. Ibid. 2019. No. 41. Art. 5700.

[5] Federal Law No. 259-FZ of July 31, 2020 "On Digital Financial Assets, Digital Currency, and the Introduction of the Amendments to Certain Laws of the Russian Federation" [O tsifrovykh finansovykh aktivakh, tsifrovoy valyute i o vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii]. Ibid. 2020. No. 31. Art. 5018.

[6] Civil Law Rules on Robotics: resolution adopted by the European Parliament on February 16, 2017. 2015/2013(INL) P8_TA-PROV (2017)0051. [2103-MS]. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (accessed:)

was responsible for his/her own area of work independently, watching, introducing corrections, using information, making decisions, now there is what might be called a partner — a robot who performs some of the tasks independently and some others, under a human being's guidance, and vice versa. Which brings us to the question: what types of decision-making should be trusted to electronic technologies, and what should remain the responsibility of governmental agencies and all public authorities. Creating typologies of administrative decisions is one of the vital academic and practical challenges because in the current electronic settings both rationales for decision-making and kinds of decisions to be made are changing.

The issues of managerial decision-making are logically tied in with the issue of liability for one's mistakes or violations of the law. An answer to this can be found in a model of shared liability, when parties liable for a robot's mistakes or even harm it has caused include the software developer who created software for the respective robot; the robot's operator responsible for its exploitation; and finally, the officer, the employee, the worker responsible for this area of work. This is a legal arrangement whereby each party carries his or her share of burden.

The legal issues invoked here should be dealt with very cautiously and accurately, seeking to strike a right balance, and moving on one step at a time, slowly because there are still too many unknowns in this new dependency between the traditional regulatory processes and the now ubiquitous processes of technization.

Introducing a new legislative framework, one should take into account the realities of the fourth industrial revolution, including fusion of technologies and erosion of the traditional boundaries between physical, digital, and biological spheres [Schwaub K., 2016]. Analyzing specifics of legal aspects of technization in economy, ecology, and biotechnology, one can see that the total or partial failure to take into account realities of life produce only superficial solutions: laws and regulations are adopted but don't really work or produce only a semblance of the desired effect, etc.

Of paramount importance is the knowledge of the dynamics of individuals' socio-legal roles and of the mechanics of adaptation of citizens, officials, public servants, entrepreneurs, pensioners to digitization — the process creating the new space where information and law overlap. The key question is whether an individual is prepared to use this space and digest the colossal volumes of diverse information, which enable people to expand the range of their activities and to better choose among different options. Hence the need to diagnose risks are an inevitable concomitant

of any human activity. When one develops legislative and regulatory instruments and performs legally important acts, risks should be assessed in advance.

2. Digitization through the lens of international law

The issue of relationship between digitization and law from the viewpoint of international and Russia's national legal systems is worth consideration.

Scientific advances accelerate the pace of global changes. International law in these circumstances becomes one of the indispensable regulators of technological progress. The ability of international law to respond to these challenges, however, is not boundless. In particular, the scope of international law and its applicability to the new technologies have some structural limitations [Rayfuse R., 2017: 500]. International public law does not have a single centralized law-making body and, therefore, lacks hierarchy. Besides, international public law is a "fragmented" legal order with a strong potential for conflict, which calls for rules to apply when addressing various possible conflicts of legal norms.

International law can serve as an organizational mechanism that countries willing to cooperate in the field of science can use. Thus, the high costs of large-scale scientific programs necessary for substantial progress in various fields of human knowledge encourage international cooperative projects and information exchange.

International organizations' activities are now an indispensable element of global politics. These organizations are parties to multilateral interactions, negotiations, global economic and financial processes, etc. In September 2018 Secretary-General of the UN presented a Strategy on New Technologies (hereinafter referred to as the Strategy), which "[defines] how the United Nations system will support the use of these technologies to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws." So, the Strategy presents the UN with a very difficult challenge: to regulate not only the past and present development and introduction of technologies, but also the indeterminate future these technologies present.

To support the Strategy's implementation, an Innovation Lab was established under the auspices of the Executive Office of the UN's Secretary-General. "The goal of the lab is to promote and support innovation across

the Secretariat, share best practices, and support efforts in the System to help incentivize and scale up existing and future innovative solutions for [the acceleration of the sustained development goals]." The Innovation Lab is also "tasked with organizing regular, thought-provoking exchanges between the Organization and outside innovators and technology pioneers." The Laboratory also "[supports] ongoing initiatives and [provides] an opportunity to scale up, where relevant."

The new technologies' technical features can open up previously unknown opportunities for strengthening the effectiveness of the provisions of international law. Can we automate international law? Moreover, can artificial intelligence systems be incorporated into the process of international law making?

The unilateral exploitation of artificial intelligence systems will undoubtedly contribute to changes in diplomacy and international negotiations in the nearest decades. For instance, yet in 2018 the ministry of foreign affairs of the People's Republic of China, to support strategic decision-making, started using an artificial intelligence, providing Chinese diplomats with a range of options and assistance in risk assessment.[7] But even if such "legal automation" is feasible for national legal systems, will this technology ever break through into the area of international public law?

First, the new technologies can be used for monitoring compliance with, and preventing violations of, international law. The ability of upgraded computerized and robotized systems to collect and process data vastly exceeds the respective human faculties. These systems can be used for documenting and analyzing data in order to identify consistent patterns that can result in violations of international law. There are some examples already proving that it is possible to significantly increase compliance with international law.

For instance, the Protection Assistant for Wildlife Security system (PAWS) now employs a machine learning algorithm predicting where poachers can show up in the nearest future. Using elements of artificial intelligence, the tool analyzes data about previous known poaching operations to suggest to wildlife rangers where illegal hunters are most likely to turn up next. Thanks to the machine-learning algorithms, the intelligence tool PAWS becomes more and more precise as new data is fed into it. PAWS uses the concepts and models of the game theory — in particular, security

[7] Available at: https://rg.ru/2018/08/02/v-kitae-sozdadut-iskusstvennyj-intellekt-dlia-diplomatov.html (accessed: 17.02.2021)

games — and an automated tool generating effective and randomized itineraries for patrol.

Another example of the use of artificial intelligence, Hala Systems' technology Sentry predicts aerial bombardment, affording time for civilians to hide in shelters. Sentry's creators point out that this is a commercial tool and they intend to offer the product in the future to public and private agencies for monitoring war zones and disaster areas.

Second, advanced technologies can be used for investigating violations of international law. In contexts of legal proceedings in international courts, blockchain can be used for checking and sharing evidence in order to ensure prosecution of international crimes [Lebedev V.M., Khabrieva T.Y., 2019: 301-342]. Most of these analytical tasks are now performed by humans, although many of them can be automated or improved using machine learning.

Third, the new technologies can be used for solving global problems. One is led to believe that cutting-edge artificial intelligence tools capable of analyzing data collected internationally will contribute to solving such global problems as climate change, sustained development, migration, terrorism, and armed conflicts.

As for legislative regulation of artificial intelligence, presently the field is dominated by private standards and guidelines produced by the industry (for instance, Google, Microsoft or Yandex). Corporate self-regulation is useful, but it still is voluntary and non-binding. Besides, not a result of governments' consensus, private standards are susceptible to influences from private interests and values. Given this, international law and international institutions can become coordinators of the efforts to develop the regulatory framework, perhaps with an eye on producing agreed-upon international principles which would ensure the integration of the core values into the design and development of the new technologies.

3. Legal personality and modern digital technologies

The modern technologies propose radical methods to transform life, so academic debates are centered on the issue of how to legally define a human being. The question that begs to be asked is this: what sort of influence do modern scientific advances have on the concept of legal personality — and, conversely, how does the corresponding legal construct can influence society's development?

The advances in informational and other technologies, in particular, reveal a new dimension of the problem of distinguishing between the human

being and the machine. The process of integration of a human body with engineering devices is called cyborgization. The cyborg (an abbreviation of cybernetic organism) is a biological organism containing mechanical or electronic components, "a hybrid of machine and organism" [Haraway D., 2017: 11]. As human beings become more dependent on mechanisms, including the substitution of organs with mechanical devices (prostheses, implants), they are gradually turning into cyborgs.

Inasmuch as law is concerned, the key questions to answer are these: what is the cyborg and what are its distinctive features; how is therapeutic cyborgization different from cyborgization intended to biotechnologically improve human beings; and what are acceptable limits to the coupling of the human being and the machine?

Identifying the boundary between the human being and the machine is not that easy because generally speaking any instrument or fixture created and used by a human being can be considered as his/her artificial extension. To identify the level of integration of a human body with technical devices when human identity becomes an issue, several criteria have been suggested: structural, functional, and the invasiveness criterion. Based on the first two criteria, the devices at issue include only structural or functional analogs of / substitutes for human organs [Yudin B.G., 2011: 18]. Yet another criterion for assessing the coupling of a human and a machine is the question of whether the device invades the person's body, whether it "[violates] a boundary between what is inside the person and what is outside" [Düwell M., Rehmann-Sutter C., Mieth D., 2008: 259].

Thus, neural prostheses can be non-invasive (electrodes stimulate electrical activity of the brain), minimally invasive (electrodes are implanted in the peripheral nervous system) and invasive (electrodes are implanted in certain areas of the brain). In the latter case, looking through the lens of the invasiveness criterion, we can see that there exists a closest connection between technologies and a human body (placing implants in the brain or the spinal cord requires a surgical intervention), and this sort of binding raises additional ethical and legal questions [Hochberg, L., Cochrane T., 2013: 235-250]. According to the guidelines of the European Group on Ethics in Science and New Technologies, "implants that cannot be easily removed" should be regulated by law as strictly as implants used in warfare.[8]

[8] Ethical Aspects of ICT Implants in the Human Body. Opinion 20. European Group on Ethics in Science and New Technologies to the European Commission. Luxembourg: Publications of the European Communities. 2005. Available at: https://ec.europa.eu/digital-single-market/en/news/ethical-aspects-ict-implants-human-body-opinion-presented-commission-european-group-ethics (accessed: 17.02.2021)

As any other biomedical technology, cyborgization is dual-purpose. Initially, the technologies are presented as opening new therapeutic possibilities: devices integrated into a human body can replace organs out of order and set right dysfunctions that can occur. As the technologies improve, however, their purpose shifts from the restorative function to the function of improving healthy persons' physical and intellectual abilities, and this raises quite different questions.

No matter how controversial, the gap between the mentioned objectives is necessary for further differentiation of the regulatory frameworks for body implants. Seemingly less problematic, incorporation of therapeutic artefacts into a human body is already partially covered by the regulatory framework concerning medical appliances. Cyborgization aimed at "improving" human beings, to the contrary, exists in a legal vacuum, although, one is inclined to think, it should be significantly restricted. The abovementioned criteria — in particular, the invasiveness criterion — can be used for differentiating between therapeutic effects of the technologies on individuals and these technologies' eugenic, upgrading effects.

Although there is some substance to the argument about a somewhat hypothetical nature of legal issues concerning the future possible application of such technologies as simulated reality, super-intellect, downloading consciousness, chemical preservation of the brain, etc., implanting artificial elements in a human body that affect its functioning is already a common practice. Presently high-tech implants are the fastest growing sector of biomedical research. Many of these implants have been widely used in healthcare for many years, forming close ties between the technologies and the organisms.

There is a wide range of implants which can be differentiated with respect to their technical characteristics and the stage of the relevant project's development (commercial use, research and development, experimental design), as well as with respect to purposes they serve (therapy, diagnostics, identification, etc.).

Cochlear and cardiac implants (heart valves, cardiac pacemakers, stents) have shown themselves to good advantage. Researchers are now working on the heart transplant, which can be used instead hearts from biological donors or at least to significantly increase the time when patients can safely wait for biological transplants. There are reasons to believe that at clinical trials the artificial heart would perform better and safer than xenotransplants, which until recently were inspiring similar hopes.[9] Along with the

[9] See: "I'm Waiting for an Artificial Heart That Will Work for a Long Time." President of the League of Nation's Health Leo Bokeria about Surgeries for 80-year-old Patients and

artificial heart, scientists are developing an artificial lung — a device to saturate blood with oxygen and remove carbon dioxide from it, assuming thus several functions of the biological lung.

The earliest body part substitutes were limb prostheses. Passive and serving an aesthetic purpose, the first prostheses were intended only as imitations of lost limbs. Next in line prostheses began to be attached to patients' bodies mechanically, as a simple substitute for a missing body part. Presently prosthetic research and development is largely focused on high-tech devices, which, integrated with the nervous system, can receive tactile signals synchronously with it and be controlled directly by the motor cortex of the brain [Stepanenko D., 2016: 26–27].

So, such devices are becoming ever more sophisticated and functional. "Recent developments in engineering technologies have meant that the ability to integrate silicon[10] with biology is reaching new levels and implantable medical devices that interact directly with the brain are becoming commonplace" [Tadeusiewicz R., Rotter P., Gasson M., 2012: 41–51]. Brain implants, brain-computer interfaces, transcranial magnetic stimulation and transcranial electrical stimulation can have a significant impact on a person's emotional, kinetic, and cognitive characteristics.

Because the brain is presumably an individual's common denominator and, therefore, the focus of transhumanist ambitions, the exploitation of such devices raises questions about admissible limits of cyborgization of human beings. Whereas there is a general support for the idea to create and use, for medical reasons, body parts' substitutes that can be repaired or replaced when out of order, the issue of cyborgization of the brain, much less the prospect of fully substituting the brain with an artificial system, is more complex. The most radical proponents argue that since generation of information is a functional basis of consciousness (functionalism), consciousness can be simply copied to a digital device and, so, there should be no legal prohibitions and restrictions on cyborgization of the brain. A more restrained approach is to recognize the necessity to preserve the material substrate of consciousness (mind-brain identity theory and certain

Rehabilitating Children After Surgeries.' [«Ya zhdu iskusstvennoe serdtse, kotoroe budet rabotat' dolgo». Prezident «Ligi zdorov'ya natsii» Leo Bokeriya — ob operatsiyakh dlya 80-letnikh patsientov i reabilitatsii detey posle khirurgicheskogo vmeshatel'stva] In: Izvestia. June 3, 2019. Available at: URL: https://iz.ru/883847/valeriia-nodelman/ia-zhdu-iskusstvennoe-serdtce-kotoroe-budet-rabotat-dolgo (accessed: 17.02.2021)

[10] The metaphor plays up the fact that this organic element is used in the manufacturing of most modern microchips. Artificial hearts and other organs are likewise manufactured from organosilicon compounds.

quantum-mind theories). Although scholarly inquiry into these questions includes, first of all, the continuing work to develop theories of consciousness, which explain the seminal issues of the relationship between mental and physical, law should be applied to this inquiry as well.

The first cautious attempts to "specify the design" of the brain and answer the question about a desirable direction for the expansion of consciousness, the question of whether certain areas of consciousness or the brain may be touched only in the case of serious psychiatric disorders or brain injuries or may not be touched under any circumstances, etc. — all of this brought about Magna Cortica: the basic guidelines for developing and introducing brain modification technologies, to be used in the years immediately ahead. Invoking, not unintentionally, the Magna Carta, Magna Cortica is a set of rights and restrictions designed to prevent potential abuses in the world obsessed with cognitive enhancement. The items include: 1) the right to self-knowledge; 2) the right to self-modification; 3) the right to refuse a modification; 4) the right to modify/refuse to modify your children; 5) the right to know who was modified.[11]

With the advancement of the technologies designed to integrate the human body or even the brain with technical devices for the purpose of restoring or even enhancing natural capabilities, there are questions inevitably being raised about the impact of these changes on the identity of such cyborgized creatures. The most radical question is probably this: to what extent does a human being remains human and, accordingly, a subject of law when his/her main external and internal organs are substituted with artificial implants or boosted with devices that enhance the person's abilities to a level unachievable for a biologically "natural" creature?

So, inasmuch as the concept of legal personality of a human being is concerned, one of the key consequences of human beings' cyborgization is the growing mismatch between the biological criteria of belonging to a species, on the one hand, and the set of characteristics that places an individual in the legal personality category, on the other.

4. Ecological imperative during the digital transformation

Broadly speaking, the relationship between the impact of digital technologies and the impact of law on the workings of society can be summed

[11] Available at: http://www.iftf.org/future-now/article-detail/from-10yf2014-magna-cortica/ (accessed: 02.02.2021)

up in three formulas: 1) law loses; 2) law lags behind; 3) law is in tune with the times.

In the first model, law's regulatory potential is less effective than digital technologies'. Improving legislation, therefore, is not tantamount to making it more effective. And the use of information technologies, for its part, lets us achieve objectives pursued by the authors of a respective legislative instrument. Besides, people find the use of digital technologies more convenient than the application of procedures prescribed by law.

An illustration for this model is the solution for the mass deaths of bees blamed on a wanton use of pesticides and agrochemicals used for eliminating agricultural pests. As is well known, in 2019 mass bee deaths were reported in several regions of Russia due to a wanton use of pesticides and agrochemicals. This is a multi-layered problem touching on the issues of state registration of pesticides and agrochemicals imported into Russia, governmental control over their use, etc. An important aspect of this story is the mandatory requirement to inform apiarists and population whenever there are plans to use pesticides and agrochemicals. In 2020 the Republic of Bashkiria proposed to enshrine in national law the requirement to inform population about instances of the use of pesticides and agrochemicals.[12] It should be noted that there is already a bylaw in place requiring that users of pesticides and agrochemicals warn population when they plan to use them.[13] This begs the question of whether we need amendments to our national legislation if the requirements of the Sanitary Rules and Norms (SanPiN) fail to ensure that population and, first of all, apiarists, are duly warned. How the public warning system can be improved?

According to media reports, Russia now has an online platform for farmers and apiarists where farmers can notify apiarists about where and when chemicals will be used, and this helps prevent mass bee deaths. It is expected that this platform will prevent mass bee deaths caused by failures to warn bee-keepers about plans to use pesticides in a timely manner. Whereas previously people tried to handle this problem using groups on social networks and in the messengers, as well as electronic message boards

[12] Draft of Federal Law No. 923742-7 " Introducing Amendments to Article 22 of the Federal Law 'On Safe Handling of Pesticides and Agrochemicals' [O vnesenii izmeneniya v stat'yu 22 Federal'nogo zakona «O bezopasnom obrashchenii s pestitsidami i agrokhimikatami»]. Available at: URL: https://sozd.duma.gov.ru/bill/923742-7 (accessed: 17.02.2021)

[13] Chief Public Health Officer of the Russian Federation. Orders No 17 March 2, 2010 "On Approving the Sanitary Rules and Norms (SanPiN) 1.2.2584-10" [Ob utverzhdenii SanPiN 1.2.2584-10] and No 40 December 2, 2020 "On Approving the Sanitary Rules and Norms (SP) 2.2.3670-20" [Ob utverzhdenii sanitarnykh pravil SP 2.2.3670-20].

and private contacts, now there is a universal platform in place. It can be accessed from any device connected to the Internet. Registering, bee-keepers need to mark a place on the map where their bee farms are located. When pesticides and agrochemicals are used on nearby plots of land, the relevant notice would be sent via email and as a text message.[14]

The digital platform will arguably make for a more efficient system of public notification about the application of pesticides than the notification methods provided for in the SanPiN. It should be noted that in late 2020 Federal Law № 490-FZ (30.12.2020) "On Bee Keeping in the Russian Federation" was adopted. This federal law has provisions regarding the prevention of the poisoning of bees by pesticides and agrochemicals (§16). Thus, no later than three days in advance of the application of pesticides and agrochemicals parties responsible therefor must notify of the event, through mass media (radio, print newspapers, electronic and other means of information and communication), residents of localities situated within seven kilometers of the border of plots of land where pesticides and agrochemicals will be used. This article of the law for the first time directly provides for the use of electronic communications for public notification, although this statutory requirement appears to lack specificity.

The second model — when law is not catching up with the developments in digital technologies — most often occurs in various spheres of legal regulation because law as the regulator of social interactions is more conservative. Such areas include, for instance, the procedures for assessing impact of industrial and other activities on the environment (hereinafter referred to as OVOS — *otsenka vozdeystviya na okruzhayushchuyu sredu*), regulated by Order No.372 (16.05. 2000) issued by the State Committee for Environmental Protection (Goscomecologia) "On Approving the Regulations on Assessing Impacts of Planned Industrial and Other Activities on the Environment in the Russian Federation." The OVOS prescriptions include giving the public notice on planned actions that can cause harm to the environment.

The order prescribes that such notice is made via the mass media: a brief notice should be printed in official publications of the federal executive bodies (for federal-level assessments), the executive bodies of the constituent entities of the Russian Federation, and the local self-governance bodies. Additional notification of participants of the OVOS can be carried out via radio, television, periodicals, the Internet, and other channels of informa-

[14] Available at: URL: https://specagro.ru/news/202005/v-rossii-zarabotala-onlayn-platforma-dlya-fermerov-i-pchelovodov (accessed: 17.02.2021)

tion delivery. The Internet thus is regarded as a secondary information delivery channel.

And the current OVOS regulations do not require to notify the public about forthcoming events by posting relevant messages on web sites of relevant public authorities. The most often used public notification method, meanwhile, is now precisely posting information and documents on public authorities' web sites and sending out information via email and the messengers.

Given this, it would seem appropriate to introduce the following provisions to the OVOS regulations: 1) the public notices about planned activities must be posted on public authorities' web sites; 2) OVOS materials should be posted online and publicly accessible; 3) an electronic log book should be kept to record advance notices about OVOS events; 4) public debates should be carried out online (as well as offline).

An interesting example of law staying in tune with digitization is the new legal institution of informational models in design and construction, which was introduced in the town planning legislation in 2019. Russia's Town Planning Code contains such term as "the informational model of a permanent building or structure construction project" — it refers to an array of interrelated data, documents and materials pertaining to a permanent building or structure construction project, which are compiled electronically at different stages of pre-construction survey and in the course of creating architectural and engineering design, building, renovating, structural repairs, exploitation, and demolition of a permanent building or facilities.

In order to introduce the informational models, several organizational and technical problems will have to be dealt with, and yet it can be assumed that the informational models will become widely used in construction design and, little by little, completely replace construction projects specs and drawing in the familiar textual and graphic formats. The informational model's key advantage over the traditional construction project drawings and specifications is the fact that the informational model accompanies its respective building/facility during the structure's entire life cycle. So, the informational model will allow to trace all transformations of the respective structure from its inception to its demolition.

Conclusion

Law steadily continues to be the regulator of socio-economic and other processes in society both at home and internationally. This is a very impor-

tant mechanism, which promotes both stability and the necessary transformational activities of individuals and public institutions.

On the other hand, digitization and the new information technologies change the nature of activities of subjects of law and the volume of their legal relations and expand the scope of their future activities.

Law meanwhile works in full force, contributing to technological progress. Law is an excellent ally to cutting-edge research and development projects, to digitization and informatization of society.

References

Artyukhin R.E., Povetkina N.A. (eds.) (2021) *New institutions of budgetary law and digital revolution*. Moscow: Norma, 192 p. (in Russian)

Bogolyubov S.A. (2020) *The development of environmental law in Eurasia*. Moscow: INFRA-M, 432 p. (In Russian)

Düwell M., Rehmann-Sutter Chr., Mieth D. (2008) *The Contingent Nature of Life: Bioethics and Limits of Human Existence*. Heidelberg: Springer, 373 p.

Engels F. (2019) *Anti-Dühring*. Moscow: AST, 480 p. (in Russian)

Haraway D. (2017) *A Cyborg Manifesto*. Moscow: Ad Marginem Press, 128 p. (in Russian)

Hochberg L., Cochrane T. (2013) Implanted Neural Interfaces. Ethics in Treatment and Research. In: *Neuroethics in Practice. Medicine, Mind, and Society*. Chatterjee A., Farah M. (eds.). Oxford: University Press, 290 p.

Khabrieva T.Y. (2016) *La réforme constitutionnelle dans le monde contemporain*. Moscow: Nauka, 223 p. (in French)

Lebedev V.M., Khabrieva T.Y. (ed.) (2019) *Justice in the Modern World*. Moscow: Kontrakt, 688 p. (in Russian)

Pilipenko A.N. (ed.) (2021) *Trends in digitalizing executive power in foreign countries*. Moscow: Infotropik, 232 p. (in Russian)

Schwab K. (2016) *The fourth industrial revolution*. Moscow: Eksmo, 400 p. (in Russian)

Rayfuse R. (2017) Public International Law and the Regulation of Emerging Technologies. In: *The Oxford Handbook of Law, Regulation, and Technology*. Brownsword R., Scotford E., Yeung K. (eds.) Oxford: OUP, pp. 500–522.

Sinitsin S.A. (2020) *Russian and foreign civil law in the conditions of robotics and digitalization. A case of interdisciplinary research*. Moscow: Infotropik, 212 p. (in Russian)

Stepanenko D. (2016) With a wave of thought. *Populyarnaya mekhanika*, no 2, pp. 26–27 (in Russian)

Talapina E.V., Yuzhakov V.N. et al. (2020) *Data circulation in state management: perspectives of legal regulation*. Moscow: Delo, 244 p. (in Russian)

Tadeusiewicz R., Rotter P., Gasson M. (2012) *Restoring Function: Application Exemplars of Medical ICT Implants. Human ICT Implants: Technical, Legal and Ethical Considerations*. The Hague: Springer, 186 p.

Yudin B.G. (2011) Borders of human existence in the world of new technology. *Working papers on bioetik.* Moscow: Gumanitarniy universitet press, pp. 4–22 (in Russian)

Data Protection Regulation and International Arbitration: Can There Be Harmonious Coexistence (with the GDPR Requirements Concerning Cross-Border Data Transfer)?

Elena Mazetova

Lecturer, Department of International Law, National Research University Higher School of Economics, LL.M. Address: 20 Myasnitsky Str., Moscow 10100, Russia. E-mail: emazetova@hse.ru

Abstract

Recent global trends are producing powerful growth in the digital environment, and its spread is prompting adoption of strict and comprehensive regulation to ensure data protection. This results in a number of difficulties, one of which is lack of consistency between data protection regulation and the regulatory regimes applicable to specific industries and institutions. That inconsistency is particularly evident in the field of international arbitration — one of the most widely used and convenient methods for resolving international disputes. The principles and fundamental concepts that largely define international arbitration, such as autonomy of the parties and confidentiality, have made its use very well accepted and widespread. However, data protection requirements often force the parties that are subject to them to make a difficult choice between the basic principles of international arbitration and the requirements of data protection regulation. This bind has come about because data protection regulation, which generally imposes comprehensive compliance obligations, rarely takes into account the specifics of the industries in which it will be applied. In this article it is analyzing application of the GDPR requirements that pertain to cross-border data transfer from the perspective of international arbitration in order to illustrate difficulties and regulatory gaps that may be encountered by the entities interested in thorough compliance with the applicable regulations.

Keywords

private data, data protection, cross-border data transfer, GDPR, international arbitration, legal claims, legal proceedings.

For citation: Mazetova E. A. (2021) Data Protection Regulation and International Arbitration (Can There Be Harmonious Coexistence?) *Legal Issues in the Digital Age,* no 2, pp. 21–48.

DOI: 10.17323/2713-2749.2021.2.21.48

Introduction

The idea that private data needs to be protected is not new: it stems largely from Semayne's case (in which it was declared that "the house of every one is to him as his castle and fortress")[1] [Cooper D., Kuner C., 2017: 44] and has undergone a lengthy path of development since then.[2] People have ultimately become much more aware of the importance of protecting their private life and, as a logical extension, of guarding their personal data, but the explosive development of technology has made protecting data a challenging task that requires consideration of various nuances.

The problems attendant upon pervasive digitalization are now being widely discussed at a time when the standard way of saving and sharing information is transitioning from paper to digital formats and most processes and communications are going online, and it is well accepted that the numerous benefits from increasing use of technology usage also entail significant risks. Undoubtedly, the trend toward digitalization has been significantly reinforced and accelerated by the COVID-19 pandemic, and it is unlikely that this progression toward a digital reality can be reversed in the future. As a result, we face a dramatic increase in the types and amount of data, including data of private individuals, which is constantly being collected, stored and transmitted on various (and also continually proliferating) types of devices [Burianski M., Reindl M., 2010: 183].

In this context it is not surprising that data protection issues are attracting increased attention from state actors,[3] which then results in the development of more advanced and complex data protection regulations.[4] It is notable

[1] See Semayne's case, 77 Eng. Rep. 194 (Kb 1604).

[2] The idea of data privacy was elaborated thoroughly by Samuel Warren and Louis Brandeis in their article of 1890 published in the *Harvard Law Review*.

[3] For example, the Brazilian General Data Protection Law. Available at: https://gdpr.eu/gdpr-vs-lgpd/ (accessed: 20.04.2021). Another example is the California Consumer Privacy Act. Available at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do (accessed: 20.04.2021)

[4] According to data from the United Nations Conference on Trade and Development, only 19% of countries across the globe have no special data protection and privacy regulations. Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed: 20.04.2021)

that the recently growing interest of states in regulating data protection issues also points up another trend in digitalization, which is the increased speed and technical simplicity of transferring data between different countries. This trend is understandably welcomed by commercial companies (in particular, those that conduct their business at the international level); however, it is causing heightened concern on the part of regulators. The upshot is that states want their data protection standards to apply across jurisdictional borders or else to significantly restrict transfers of data across those borders [Cooper D., Kuner C., 2017: 32–33, 72], and this influences the approaches to data protection legislation adopted by the respective states.

It is also noteworthy that, although large IT corporations such as Google or Facebook are seen as the main "addressees" of recent data protection regulation, we find that even companies whose main business is not directly related to the internet or development of technology are facing significant fines for violation of data protection laws.[5] Thus, it is fair to say that data protection regulation is becoming truly comprehensive and influencing almost all areas of life by requiring the key actors responsible for collecting and processing private data to apply additional safeguards and protections.

As will be shown below, all these circumstances have led to conflicting requirements, not only within the field of data protection itself (and in particular as it affects cross-border aspects) but also between data protection regimes and other areas of law, e.g. international arbitration. Those areas of law normally have their own rules and principles of operation, but at the same time they are not exempt from the application of data protection requirements. As Christopher Kuner correctly indicated, this incompatibility between different legal regimes may "go beyond simple conflict of laws, and can be viewed as conflicts between different social sectors" (Kuner C., 2013: 135).

International arbitration provides a good example of this kind of conflict: first, it is a rapidly developing and widely used tool for resolving international disputes. Almost any company that conducts business across borders has either already resorted to international arbitration in order to resolve disputes or may potentially need to do so.[6] Second, although inter-

[5] For example, a £18.4 million fine was imposed on Marriott International Inc. for a data protection breach (ICO Penalty Notice. 30 October 2020, case ref.: COM0804337. Available at: https://ico.org.uk/action-weve-taken/enforcement/marriott-international-inc/ (accessed: 06.04.2021)). A similar fine of £20 million was levied against British Airways (ICO Penalty Notice.16 October 2020, case ref.: COM0783542. Available at: https://ico.org.uk/action-weve-taken/enforcement/british-airways/ (accessed: 06.04.2021)

[6] International arbitration was considered the preferred method of dispute resolution by 97% of respondents to the 2018 International Arbitration Survey: The Evolution of In-

national arbitration understood as a branch of law is far removed from the field of data protection, it is still significantly affected by it and in practice is often forced to adapt to data protection rules.

In the analysis that follows, we will focus on the application of data protection regulations to international arbitration and will consider certain difficulties and inconsistencies that parties to international arbitration may encounter in their attempt to comply with data protection requirements.

1. How data protection regulation affects international arbitration

As mentioned above, the growing concern about data protection could not fail to impact nearly every aspect of life and business operations.[7] Because international arbitration is one of the most commonly used and convenient methods for resolution of international disputes, it should come as no surprise that it was affected both by the application of regulations concerning cross-border data transfer and also by the current trend toward data protection in general.

The impact becomes even more significant due to the recent development of online arbitration, as well as to the increasing penetration of digital tools and techniques into the conduct of arbitration proceedings.[8] Furthermore, the risks associated with cross-border data transfer become very meaningful in practice when international arbitration brings together participants from different jurisdictions who travel across the world and represent companies from different countries [Pastore J., 2017: 1029]. Each and every of those participants may be exposed to risks that could undermine the entire arbitration process [Cohen S., Morril M., 2017: 1005].

Although it may be argued that those risks are limited by the inherent confidentiality of arbitration and also by a consent-based and generally balanced approach to the production of documents and information in arbitration [Born G., 2021: 2495–2496], experience shows that international

ternational Arbitration, which was conducted by the School of International Arbitration at Queen Mary University of London in partnership with White&Case LLP.

[7] For instance, question related to the GDPR influence over the arbitration was one of those that the tribunal had to evaluate in *Tennant Energy LLC* v *Government of Canada* (see: *Tennant Energy, LLC* v *Government of Canada*, PCA case No. 2018-54).

[8] The Queen Mary University survey also shows that at least 61% of respondents highlight the "increased efficiency, including through technology" and that such measures as videoconferencing and hearing room technologies are always or frequently used by over 60% of respondents.

arbitration, as well as the parties involved in it, are encountering instances of data breaches with increasing frequency. The risks are incurred in a wide range of circumstances that include mistakenly sending personal information of one of the parties to a person not connected with the proceedings [Smeureanu I., 2011: 183–184],[9] leakage of clients' private data from law firms [Cohen S., Morril M., 2017: 987]; along with targeted hacker attacks on arbitration institution (e.g., as happened to the Permanent Court of Arbitration in the Hague in July 2015 in the course of hearing *The Republic of the Philippines* v *The People's Republic of China*) (Pastore J., 2017: 1023, 1026).

The risks to which private data may be exposed[10] in the process of international arbitration — which is clearly not risk-free — are a sufficient practical justification of applying data protection measures.

The need for the entities involved in international arbitration to comply with data protection requirements arises also from the data protection laws themselves. First, laws in that field typically offer a definition of "data processing" (as an activity which entails application of data protection regulation) so broad that almost any activity or process occurring in the course of resolving a dispute by an arbitration tribunal, from taking initial evidence to issuing an arbitral award, may fall within the scope of data protection requirements[11] and so trigger specific compliance obligations.

Second, although most of the recent data protection requirements exempt judicial proceedings from some group of obligations or from specific obligations, arbitration is not mentioned explicitly.[12] It is difficult to understand the reasoning behind this approach (there are as yet no official

[9] See, for example, the claim of an individual, Mr. Carlos Antonio, brought against an arbitration institution in Spain. As a result of a data breach, the arbitral institution was fined €6,000 for infringement of its obligation to protect data and confidentiality.

[10] It should be noted that a risk-based approach is also suggested by data protection regulations themselves, such as the GDPR, which highlights the importance of evaluating risks. Available at https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ (accessed: 10.04.2021)

[11] For example, in according with Art. 4(2) of the GDPR "processing" is defined as "any operation … which is performed on personal data…, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[12] See, for example, Art. 23(f) of the GDPR; also see discussion of the Indian Draft Personal Data Protection Bill. Available at: http://arbitrationblog.kluwerarbitration.com/2019/04/16/data-protection-in-india-and-arbitration-key-questions-ahead/ (accessed: 23.04.2021)

comments or guidance that would explain it), but it leads naturally to discussion of the applicability of the existing exceptions to arbitration due to its mixed nature, which combines jurisdictional and contractual features [Lew J., Mistelis L., Kroll M., 2003: 72]. Nevertheless, commentators generally agree that a conservative approach which interprets the term "judicial proceedings" in a narrow sense as covering only state courts should prevail [Paisley K., 2018: 857].

As matters now stand, parties to arbitration cannot rely on the general exceptions and are forced to apply more nuanced, case-by-case analysis in order to properly comply with data protection regulations.

As a result, many reputable and respected arbitration institutions regularly update their rules and recommendations to the parties and tribunals involved in order to properly address data protection considerations.[13] Parallel to that, the professional community of lawyers are working on determining the best practices to ensure accurate and comprehensive compliance.[14] The importance of those efforts cannot be overestimated: the ICCA-IBA Roadmap to Data Protection in International Arbitration indicated that it is intended "to help arbitration professionals better understand the data protection and privacy obligations to which they may be subject in relation to international arbitration proceedings".[15] Nevertheless, the broad question of whether international arbitration and data protection regulations can coexist in harmony remains open. As will be further illustrated by the example of the EU's General Data Protection Regulation (hereinafter GDPR),[16] the lack of clarity on this matter means that the that parties to international arbitration and the other participants in it must continually choose between non-compliance (or at least improper compliance) with

[13] See, for example, Art. 30A of the LCIA Arbitration Rules 1 October 2020; or Section D "Protection of Personal Data" in the ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration.1 January 2019.

[14] See, for example, the Cyber Security Guidelines from the IBA's Presidential Task Force on Cyber Security, October 2018. Available at: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (accessed: 23.04. 2021); the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration, 2020. Available at: https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html (accessed: 20.04. 2021); the Consultation Draft of the ICCA-IBA Roadmap to Data Protection in International Arbitration, February 2020. Available at: https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration (accessed: 20.04.2021)

[15] See the ICCA-IBA Roadmap to Data Protection in International Arbitration, p. 1.

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

data protection requirements and securing all the potential benefits of international arbitration.

2. How the GDPR rules on cross-border data transfer affect international arbitration

It is pertinent to note that the recent global trends in data protection regulation have been set in motion largely by the GDPR, which entered into force in 2018.[17]

The worldwide acquiescence to the GDPR is due not only to the heavy fines (up to 4% of global gross revenue or €20 million) and possible criminal liability for violation of the GDPR, but also to its broad application and potentially extraterritorial effect.[18] The EU Commission made clear the extraterritorial ambition of the GDPR when it stated that "the primary purpose of these rules is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data".[19] The approaches employed by the GDPR have also been adopted and reproduced in the legislative acts of other countries [Cooper D., Kuner C., 2017: 48). In a sense, the GDPR has prompted extensive reconsideration and improvement of data protection regimes in general, and it still remains one of the most comprehensive and detailed regulatory tools for personal data protection.

For this reason, we will examine in detail some of the data protection issues in international arbitration that have resulted from the rules promulgated by the GDPR. It should be noted that the overall impact of data protection regulation on international arbitration is significant and that it affects a wide variety of procedural matters, such as additional obligations for arbitrators and arbitral institutions [Cohen S., Morril M., 2017: 997–1002], issues with production of evidence [Cooper D., Kuner C., 2017: 100], difficulties with publication of awards [Tshanz P.-Y., 2006], etc. However, in this article we will primarily focus on analysis of the rules and grounds for cross-border data transfer: this regulatory nexus is particularly interesting

[17] The GDPR replaced the previous Data Protection Directive (Directive 95/46/EC), which had been in effect since 1995. See: The History of the General Data Protection Regulation. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (accessed: 04.05.2021)

[18] Communication from the EU Commission to the European Parliament and the / Council, Exchanging and Protecting Personal Data in a Globalised World, COM/ 2017/07 final. 10.01.2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/? uri= COM%3A2017% 3A7%3AFIN (accessed: 29.04.2021) (hereinafter EU Communication).

[19] Ibid.

because it highlights the underlining ideas peculiar to each of the regulatory fields under consideration while it also exposes discrepancies even at this basic conceptual level. We find several reasons for this particular problem.

First, the GDPR maintains that, once private data of EU data subjects is involved, data protection compliance may be required from almost everyone engaged in a case, including the principal parties themselves, counsels acting on their behalf, arbitral institutions (when applicable), members of the arbitral tribunal, and so on regardless of the home jurisdiction of any of these participants [Paisley K., 2018: 854].

Second, applying specific data protection rules, including the GDPR, in international arbitration is complicated by jurisdictional diversity, such that one party may be from one of the EU countries and another from Africa, the arbitral institution may be seated in an Asian country, the tribunal is composed of three arbitrators from three different jurisdictions, and hearings take place in various locations, etc. These geographically and jurisdictionally fragmented features of international arbitration mean that rules for cross-border data transfer will inevitably apply to international arbitration, but those rules will also be applied differently in each individual episode of data transfer.

Presumably, analysis of the cross-border data transfer regulations and identification of those that are applicable to a given situation should be the first step in preparing for arbitration, as it would determine the scope of possible disclosure and the sequence of actions required to comply with data protection regulations. It would be reasonable to expect that this first step should be rather straightforward and provide the parties with clear guidance concerning the applicable rules and potential risks. However, as will be demonstrated below, the reality may differ from expectations.

General GDPR requirements for cross-border data transfer

The GDPR regulates cross-border data transfer (i.e. transfer of data outside the European Economic Area [EEA])[20] and application of its rules in international arbitration is difficult to avoid. Requirements of the GDPR may come into play in various scenarios: for instance, when a party, either as a result of being registered within the EU[21] or due to processing or con-

[20] Actual list of the EEA countries available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European_Economic_Area_(EEA) (accessed: 10.06.2021)

[21] See Art. 3 of the GDPR.

trolling data of EU individuals,[22] must decide whether to use or disclose documents containing that data to a tribunal (be it as a part of the party's written submission, evidence requested by the tribunal, or in any other form); or perhaps that data is to be disclosed to the opposing party from a different jurisdiction so that a suitable justification for transferring that data would be required.

In dealing with these issues in international arbitration, the parties should keep in mind the complex data protection environment created by the GDPR, which consists of a combination of prohibitions, limitations and data protection standards in which each layer is important for legitimate cross-border data transfer [Paisley K., 2018: 854–855].

The general rule provided by the GDPR is based on prohibition of data transfer outside the EEA, except for a limited number of circumstances in which it is expressly permitted.[23] In fact, a list of those limited occasions (or grounds) established by the GDPR may be divided into general restrictions[24] and specific derogations [Paisley K., 2018: 878–881].[25] In addition, the GDPR establishes the specific requirement to adhere to the data protection standards irrespective of the justification employed for data transfer.[26]

The list of grounds that make cross-border data transfer permissible is provided in Articles 45–49 of the GDPR. The method for applying these grounds follows the so-called "cascade principle" [Paisley K., 2018: 878], meaning that each ground for data transfer is to be analyzed one by one and each one applied only if the preceding one was found not suitable.

The first group of grounds for cross-border data transfer contains general restrictions and is at the top of this hierarchy. It contains two requirements: first, there should be what is termed an adequacy decision; and, second, appropriate safeguards should be applied (the first of these two requirements takes precedence over the second).

Therefore, transfer of data to a third country which has an adequacy decision from the EU Commission holds the first rank in the overall hierarchy of grounds for permitting cross-border data transfer.[27] An adequacy decision in favor of a country means that the EU Commission, after scru-

[22] Ibid. Art. 2.

[23] Ibid. Art. 45.

[24] Ibid. Art. 45–47.

[25] Ibid. Art. 49.

[26] Ibid. Art. 44.

[27] Ibid. Art. 45.

tinizing a country's legislation concerning data protection, has concluded that the regulations adopted in that country offer the same level of commitment to data protection as that established within the EEA.[28] As the EU Commission has noted, if an adequacy decision is in place with respect to certain country, then data transfer to that country does not require any further safeguard.[29] In practice, however, reliance on adequacy decisions has several drawbacks (especially for arbitration).

First, adequacy decisions have at present been issued to relatively few countries,[30] which means coverage by adequacy decisions may often be incomplete when many jurisdictions are involved in data exchange. As already mentioned, arbitration often involves various jurisdictions in which data may be transmitted in the course of arbitration proceedings, and it may be difficult (if not impossible) to create an environment fully covered by adequacy decisions.

Second, having an adequacy decision is not a permanent guarantee: in fact, even after an adequacy decision in favor of a certain country has been made, that decision may be rescinded if the actual operation of its data protection system is found to be unsatisfactory.[31] One of the most striking examples of reconsideration of data transfer regimes based on adequacy decisions is in a series of cases recently considered by the Court of Justice of the European Union (hereinafter CJEU) pertaining to invalidation of the data protection regimes agreed to between the EU and the USA (i.e. the U.S.-EU Safe Harbor Framework and the EU-US Privacy Shield regime).[32]

---

[28] Handbook on European Data Protection Law,,.European Union Agency for Fundamental Rights and Council of Europe. Luxembourg, 2018 (hereinafter Handbook on European Data Protection Law), p. 254.

[29] EU Commission website. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed: 14.04.2021)

[30] The list of the countries that have adequacy decisions is available on the EU Commission website and includes: Andorra, Argentina, Canada (as concerns commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. Available at: *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en* (accessed: 04.05.2021)

It should be noted separately that until 16 July 2020 the adequacy decision regulating transfer of data between the EU and the USA was in effect (although it had limited scope). Available at: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en (accessed: 04.05.2021)

[31] Handbook on European Data Protection Law, p. 189.

[32] For more details see the press release of the EU Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield".

The first case (*Maximilian Schrems* v *Data Protection Commissioner* {"Schrems I"]),[33] was considered before the GDPR had been issued. Nevertheless, analysis of adequacy decisions provided there may also be relevant to post-GDPR practice. In this decision the CJEU invalidated the EU-US Safe Harbor regime,[34] and proclaimed that:

> [A] decision…by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State,…, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[35]

This decision had a far-reaching impact and led to a revision of data security standards between the EU and the USA. In particular, the EU-US Safe Harbor regime was reconsidered [Graham N., Mehta T., 2015] and replaced by the EU-US Privacy Shield.[36]

The second case (*Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems* ["Schrems II"])[37] resulted in the invalidation of the EU-US Privacy Shield specifically because USA domestic law granted rights of access to private data for USA public authorities; this meant that the necessary data protection could not be ensured.[38] The EU

Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 (accessed: 22.04.2021); and the press release of the Court of Justice of the European Union, No 91/20. 16.07.2020. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (accessed: 22.04.2021)

[33] See the Judgment of the CJEU (Grand Chamber) of dated 06.10.October 2015 in Case C362/14 (hereinafter Case C-362/14).

[34] In accordance with the "safe harbor" regime, US companies were able to self-certify their compliance with the agreed data protection requirements, which would simplify transfer of data from the EEA to those companies (See: EU Commission Memo/00/47 dated 27 July 2000. How will the 'safe harbor' arrangement for personal data transfers to the US work? Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_00_47 (accessed: 04.05.2021)

[35] See Case C-362/14, para 66.

[36] EU Commission press release. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. 02.02.2016. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 (accessed: 04.05.2021)

[37] See Judgment of the CJEU (Grand Chamber) of 16. July 2020 in Case C-311/18 (hereinafter Case C-311/18).

[38] See Case C311/18, para 185.

and USA have recently been in negotiations concerning a new regulatory regime which would be more in line with the principles and standards of the GDPR.[39] Until such a regulatory regime is agreed upon, companies may consider resorting to various other grounds for the transfer of data between the EU and USA, insofar as such grounds are available to them.

These cases demonstrate that adequacy decisions cannot be considered as an entirely stable ground for cross-border data transfer (the EU-US Privacy Shield was in effect for only four years before it was also invalidated); and even if adequacy decisions are in place, they can hardly be relied upon in isolation from the actual data protection measures operating in a particular country.

For the purpose of arbitration, both the poor geographical coverage of data protection decisions and the risk of a change in the status of an adequacy decision make this tool practically useless in international arbitration and force the parties to continue making their own analysis of the data protection issues in each case.

According to Art. 46 of the GDPR, transfer of data to a third country is allowed subject to the existence of "appropriate safeguards", including enforceable rights and legal remedies for the data subject.[40] The appropriate safeguards are specifically defined by the GDPR in a list that contains such instruments as binding corporate rules,[41] standard data protection clauses[42] and approved codes of conduct.[43] When applying these principles to justify data transfer in arbitration, it is important to keep in mind at least two specific features attached to these instruments.

First, almost no deviations from the established scope of commitments imposed on the entity that is handling data are allowed, as this scope is set by the EU Commission or supervisory authority acting in each EEA country.[44] The commitments established by these instruments may be regarded as

[39] See Joint Press Statement by European Commissioner for Justice Didier Reynders and US. Secretary of Commerce Gina Raimondo. 25 March 2021. Available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 (accessed: 21.04.2021)

[40] See Art. 46 and Recital 108 of the GDPR.

[41] Ibid. Art. 46 (2)(b) .

[42] In accordance with the provisions of the GDPR (Art. 46 (2)(c) and (d) of the GDPR) data controllers can choose between standard data protection clauses or "ad hoc" data protection clauses. If ad hoc clauses are to be applied, they should be specifically approved by a competent authority.

[43] Ibid. Art. 46(2)(e).

[44] See Art. 46 (2)(a) of the GDPR.

burdensome for the party receiving data[45] and inconvenient for international arbitration, especially in cases where the data recipient's "interaction" with data does not constitute a long-term established practice, but is instead the result of being involved in a particular case (e.g. as an arbitrator dealing with documents provided by the parties). A similar approach and analogous difficulties are also typical of the other types of appropriate safeguards.

Second, each instance of application of any of the appropriate safeguards requires a separate approval procedure,[46] which significantly complicates the overall compliance process and also leaves parties with almost no flexibility to arrive at terms that they are comfortable with themselves. Although employing these appropriate safeguards may seem a good solution for international arbitration at first sight,[47] their detailed provisions, which are almost completely fixed, make this ground for cross-border data transfer difficult to employ [Rosenthal D., 2019: 830].

Application of derogations allowing data transfer in international arbitration

Overview of derogations

In a situation when neither adequacy decisions nor appropriate safeguards can be applied, grounds from the second group (i.e. specific derogations) are to be considered for cross-border data transfer. The list of derogations is provided by Art. 49 of the GDPR, and it describes exceptional situations in which data transfer is allowed without either an adequacy decision or appropriate safeguards being in place. In effect, derogations are next in line under the previously mentioned cascade principle for applying grounds. The cascade principle presupposes the superiority of adequacy decisions and appropriate safeguards over specific derogations.[48]

An important consideration here is that, although application of Art. 49 of the GDPR allows cross-border transfer of data in exceptional situations, it does not negate the general obligation of a transferring party to comply with

[45] Detailed obligations are provided in 2021/914: Commission Implementing Decision (EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[46] See Art. 40, 42 and 47 of the GDPR.

[47] The European Data Protection Board Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 25 May 2018 (hereinafter Guidelines on derogations), pp. 3-4.

[48] Art. 49(1) of the GDPR.

other requirements of the GDPR.[49] In particular, Art. 44 as well as Recital 101 of the GDPR stipulate that international data transfer is to be conducted "subject to the other provisions" of the GDPR and, what is even more important, require that "the level of protection of natural persons …should not be undermined".[50]

In contrast with data transfer performed under adequacy decisions or appropriate safeguards, resort to derogations is legitimate only if data transfer takes place occasionally and does not constitute a stable channel for data transmission.[51] This peculiarity makes derogations difficult to rely on in the ordinary course of international business; however, for international arbitration this requirement is normally met. Even if company is a frequent participant in arbitration or if these rules are applied to arbitral institutions (which constantly deal with data exchanged between parties and tribunals), each particular transfer of data within arbitration occurs on an ad hoc basis and can scarcely be regarded as continuous data transmission between the entities (be they the disputing parties, the arbitrators or the arbitral institution).

The list of available derogations is closed and includes the following situations that permit cross-border data transfer:[52]

there is explicit consent to the proposed transfer;

the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

the transfer is necessary for important reasons of public interest;

the transfer is necessary for the establishment, exercise or defense of legal claims;

the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

---

[49] Guidelines on derogations, p. 3.

[50] Recital 101 of the GDPR. A similar passage is in Art. 44 of the GDPR.

[51] This requirement comes from the literal interpretation of the Recital 111 of the GDPR, which specifies that data transfer under derogations is possible *"…where the transfer is occasional…"*

[52] Art. 49(1)(a)-(g) of the GDPR.

the transfer is made from a register which is publicly available or available to persons who can demonstrate legitimate interest in consulting it;

the transfer serves the legitimate interests of the transferring party

It is apparent that not all of the derogations listed above are applicable in principle to arbitration; however, some of them may seem to be particularly suitable for it. In particular, if cross-border data transfer is required within international arbitration proceedings, the following derogations may be pertinent: having explicit consent; data transfer necessary for the establishment, exercise or defense of legal claims; or data transfer based on legitimate interest [Paisley K., 2018: 881]. Each of these grounds has its own distinctive features, and they should be considered separately.

Application of the explicit consent derogation in arbitration

Because arbitration is by nature a consensual procedure, the explicit consent derogation provided by the GDPR may seem the most logical solution, but reliance on this ground in international arbitration may be difficult in practice. The chief difficulties in resorting to this derogation arise from the GDPR requirements themselves.

The general requirements for what constitutes a data subject's consent and how it should be obtained in order to comply with the GDPR are established by Art. 4(11) and Art. 7 of the GDPR, as well as by clarifications in Recitals 32, 42 and 43 of the GDPR. In accordance with these rules data subject consent is to be freely given, specific, informed, and unambiguous.

Compliance with these requirements in the context of arbitration will have its own peculiarities. In particular, arbitration may be concerned with different types of data (sometimes even in the course of a single proceeding or one cycle of data exchange). It may involve data about employees, contractors, customers, partners, etc. [Paisley K., 2018: 870]; and in each case compliance with the GDPR principles will require different actions.

To cite one example, the transfer of an employee's data within arbitration proceedings (which is presumably the most frequent kind of data processed by the parties) may diverge from as many as three of the four requirements established by the GDPR. It may be difficult to ensure sufficient specificity[53]

[53] In particular, Recital 39 of the GDPR states that the "specific purpose should be explicit… and determined at the time of the collection of the personal data". Therefore, it is questionable whether general language regarding possible data transfer for the purposes of arbitration will be sufficient to ensure compliance.

and also compliance with the requirement of informed consent (especially when it comes to the analysis of consents obtained preemptively).[54] In particular, a conflict may arise between the level of detail required for an appropriate consent and the expected level of confidentiality in arbitration. It is also important to note that the GDPR requires that the data subject be "informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards",[55] which means that at the time when consent is received there should at least be an understanding regarding the scope of data importing jurisdictions.[56] Needless to say, this requirement is difficult to comply with until the arbitration has commenced. At the same time, if data subject consent is obtained on a case-by-case basis through a separate statement referring to a specific dispute or even to a specific operation occurring in the course of proceedings, which would probably better meet the GDPR requirements, the principle of confidentiality of arbitration may be compromised [Paisley K., 2018: 908].

Furthermore, there may be an "imbalance of power" between the employer and employee[57] that comes into conflict with the GDPR requirement of "freely given consent"[58] (e.g. the quality of consent may hinge on whether an employee actually has an option to reject a clause in the agreement).[59] Another important consideration is that establishing the data subject's consent as freely given in complex proceedings where each operation constitutes a separate act of data processing (e.g. submission of documents, consideration of witness statements, exchange of positions between the parties, writing an award etc.) [Paisley K., 2018: 845-846) requires that

---

As another example, the issue of specificity was taken up by the Commission Nationale de l'Informatique et des Libertés (CNIL), which is the French data protection authority. Its decision dated 21 January 2019 levied a fine of €50 million against Google LLC. One of the violations that Google was accused of was a lack of valid consent to data processing. In particular, the CNIL maintained that in order to consent to the privacy policy users had to give their consent not for specific purposes, but for all the processing operations. The CNIL position was that such consent was "neither specific nor unambiguous". Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed: 15.04.2021)

[54] The European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1. dated 04 May 2020 (hereinafter Guidelines on consent), p. 7.

[55] Art. 49(1)(a) of the GDPR.

[56] Guidelines on consent, p.8.

[57] Ibid. P. 9.

[58] Ibid. P. 7.

[59] Article 29 of Data Protection Working Party, Opinion 2/2017 on data processing at work. 8 June 2017, para 6.2, p. 23.

the data subject have the option to consent to each operation separately or only to some subset of operations.[60]

Application of this rule in arbitration will mean literally that a data subject (who is normally not a party to arbitration but an employee of a party as in our example) should be provided both with information about each step of the arbitration proceedings and also should have a certain degree of influence over the procedure itself, which may lead to interference with such basic arbitration concepts as confidentiality and autonomy of the parties [Lew J.,, Mistelis L., Kroll M., 2003: 523].

This is just one specific example to show that resorting to the derogation based on the data subject's consent is a more complex matter than it might initially seem.

Furthermore, the stipulation in Article 7 of the GDPR that any consent given should be revocable at any time and that the data subject is to have the option to withdraw their consent in a manner which is as easy as giving consent is important. Thus, it follows from the GDPR's conditions for obtaining a data subject's consent and using it (and the same conclusion has been emphasized by the European Data Protection Board) that properly obtained consent gives the data subject full control over the way their date is processed and even over whether it can be processed.[61] Although this approach is reasonable in the context of data protection, it may obstruct efficient resolution of a dispute when it is applied to international arbitration.

Finally, because the data subject's consent is regarded as an exceptional rather than a standard ground for cross-border data transfer, there is a presumption of heightened risk hanging over the data subject due to the lack of adequate (i.e. analogous to the GDPR) protections.[62] In these circumstances the GDPR sets an even higher standard for the data subject's awareness of potential risk, which is why consent to cross-border data transfer must be "explicit".[63] This requirement presupposes expression of consent in a much clearer form, which also implies that more details concerning data processing operations are to be provided to the data subject.[64]

Compliance with these requirements is essential to ensure that cross-border data transfer based on the data subject's consent is lawful, and fail-

[60] Recital 32 of the GDPR.

[61] Guidelines on consent, p. 5.

[62] Ibid., p. 20.

[63] Art. 49(1)(a) of the GDPR.

[64] Guidelines on consent, p. 20.

ure to meet the requirements will incur a challenge to data transfer and significant fines.[65] Therefore, if a party chooses to collect the data subjects' consents for transfer of their data outside the EEA, that party should make sure that the standards set by the GDPR are accurately met. This exercise is not easy in itself, and it becomes even more difficult for arbitration, as the requirements of the GDPR may come into conflict with the requirements and basic concepts that are peculiar to international arbitration.

Application of the legal claims derogation

One more ground for cross-border data transfer which may be employed for the arbitration is provided by Art. 49(1)(e) of the GDPR. This provision states that transfer outside the EEA is allowed when "…necessary for the establishment, exercise or defence of legal claims". Recital 111 of the GDPR further clarifies that the legal claims derogation covers a wide range of proceedings, "whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies." The term "out-of-court procedure" implies that the legal claims derogation may also cover arbitration [Paisley K., 2018: 880].

Nevertheless, a party applying this derogation should take into account that, in accordance with Art. 49(1)(e) of the GDPR, the lawfulness of cross-border data transfer in these cases will depend upon whether the data transfer is actually "necessary" — i.e. there must be compliance with what is termed the "necessity test".[66] This test requires analysis of the data in question and of its relevance to the specific legal proceedings,[67] and thus it coheres with major principles of data protection that have been established elsewhere in the GDPR such as "purpose limitation"[68] and "data minimization".[69]

Application of the necessity test has several implications in practice. In particular, it restrains the data controller (which may be a party to a dispute

[65] In accordance with Art. 83(5)(a) of the GDPR, the fine for a breach of "the basic principles for processing, including conditions for consent…" may be up to €20,000,000 EUR or up to 4 % of the total worldwide annual turnover of the breaching entity for the preceding financial year.

[66] If Art. 49(1) of the GDPR is interpreted literally, the legal claims derogation would not be the only one subject to the necessity test. The same language is also used for the derogations provided by Articles 49(1)(b), (c), (d) and (f). (See Guidelines on derogations, p. 12).

[67] Ibid., p. 12.

[68] Art. 5(1)(b) of the GDPR.

[69] Ibid. Art. 5(1)(c).

submitted for arbitration) from transferring all the data that is potentially relevant to the legal proceedings[70] and requires limiting that data to what is directly related to the proceedings.[71] Depending on the stage in the arbitration proceedings, compliance with this rule may be challenging. When certain data, or a document containing that data, is specifically requested from a party, its relevance and necessity may be relatively easy to verify. However, when the data is included in a memorandum or any other procedural document introduced by a party voluntarily, it may require a more careful and detailed explanation of the usage of the data in question.

There are many practical recommendations that can help the transferring party in complying with these rules (for instance, the party might consider the feasibility of transferring anonymized or pseudonymized data, etc.).[72] But it is important in any case for the transferring party to understand that applying this ground will mean managing both the risk of noncompliance with the GDPR requirements (if the party fails to confirm the relevance or necessity of the transferred data to a particular dispute) and also the risk of providing insufficient evidence to succeed in arbitration (if the party takes a conservative position concerning amount of data to transfer).

This allocation of risks (or more precisely, assigning all risks to the transferring party) reveals another interesting peculiarity when the GDPR is applied to international arbitration. For example, a regulatory framework for arbitration may allow document production in principle [Born G., 2015: 186], while the decision on the relevance and necessity of certain documents will be taken by the tribunal (although with due consideration of positions of the parties).[73] A decision by the tribunal may contradict the party's evaluation of the same matter and present the party with the

[70] Guidelines on derogations, p. 12.

[71] This principle is also highlighted by Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil Litigation. 11 February 2009, p.10.

[72] Guidelines on derogations, p. 12.

[73] For example, Art. 3(7) of the International Bar Association Rules on Taking Evidence in International Arbitration (as adopted by a resolution of the IBA Council 29 May 2010), provides: "The Arbitral Tribunal may order the Party to whom such Request is addressed to produce any requested Document in its possession…". A similar approach is followed by Art. 27(4) of the UNCITRAL Arbitration Rules (as revised in 2010) establishing that "the arbitral tribunal shall determine the admissibility, relevance, materiality and weight of the evidence offered"; as well as by the majority of arbitration rules (see for example: Art. 19.2 of SIAC Rules 2016; Art. 22.2 of HKIAC Rules 2018, Art. R-34(b) of AAA Commercial Arbitration Rules and Mediation Procedures, etc.).

difficult choice of which requirements to comply with. Furthermore, the GDPR in Art. 48 establishes separate rules for transferring data in response to foreign judgements or decisions. This dichotomy within the GDPR itself points to another important issue that affects the legitimacy of cross-border data transfer: the interplay between Art. 48 of the GDPR, and the legal claims derogation.

Interplay between Art. 48 of the GDPR and the legal claims derogation

Art. 48 of the GDPR refers to situations in which transfers or disclosures are not authorized by EU law. Parties should refrain from transferring data in response to a court judgment or decision of a third country if the judgement or decision requiring data transfer is not "based on an international agreement…between the requesting third country and the Union or a Member State". Art. 48 of the GDPR broadly characterizes the bodies that may issue such judgements as courts, *tribunals* and administrative authorities. This makes Art. 48 analogous to Art. 49(1)(e) of the GDPR, as it also would extend to arbitration.

Art. 48 would then provide an answer the question about appropriate grounds for data transfer by specifying that the transfer is to be requested by a competent authority (which would be an arbitral tribunal for the purpose of this article) as well as outlining the requirements to be followed in these matters.

The explication of GDPR Art. 48 provided in the "Guidelines on derogations" states that requests for data transfer from bodies of the types permitted (for our purpose, arbitral tribunals) are not "in themselves legitimate grounds for data transfers".[74] Whether cross-border data transfer in these cases is permissible depends on two factors: first, there must be an international agreement between the two countries (the country of the authority making the request and the country of the party making a disclosure); and second, there must be a level of data protection consistent with the GDPR.[75]

In practice Art. 48 of the GDPR may provide the transferring party with two options for responding to a judgement or decision requiring data transfer outside the EEA depending on whether or not there is an agreement between the countries in question:

[74] Guidelines on derogations, p. 5.

[75] See Recital 115 of the GDPR.

if there is an agreement between the European Union or the corresponding member state and the country of the requesting authority, refer the authority making the request to the procedure for international cooperation established by that agreement (e.g., mutual legal assistance treaties);[76]

if there is no such agreement, find other grounds to justify data transfer among those that are offered by the GDPR, usually in Art. 49.[77]

This solution follows from the official guidelines on GDPR application[78] and comes from Art. 48, which stipulates that it is to be applied "without prejudice to other grounds for transfer". However, on closer examination and especially in employing this solution for arbitration, a number of questions arise.

First, it is well-known that international agreements on legal assistance between states do not common for arbitration [Paisley K., 2018: 875]. That lack may make it difficult to ascertain whether Art. 48 of the GDPR will be useful in arbitration (at least until appropriate international agreements between states come into play). However, even if we suppose that there are bilateral or multilateral treaties as envisaged by Art. 48 that pertain to arbitration, that will not automatically settle the issues in applying Art. 48. At a bare minimum, there would still be the question of how to determine the nationality of an arbitration proceeding, as this may be important in understanding which specific international agreement to apply. For national courts and for administrative or investigative authorities, the jurisdictional link is immediately apparent; but for international arbitration the boundaries are blurred. This has become quite evident with the advent of the concept of delocalized arbitration, which presupposes that international arbitration is detached from any national legal system [Lew J., 2006: 179–204].

Although one possible solution could be reliance on the seat of the arbitration[79] by analogy with the approach most commonly taken to determine the nationality of an award under New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (hereinafter New York

[76] Guidelines on derogations, p. 5.

[77] See Recital 115 of the GDPR; Guidelines on derogations, p.5.

[78] Guidelines on derogations, p. 5.

[79] It should be noted that even for purposes of enforcement, the seat of arbitration is not the only possible criterion. For instance, the wording in Art. I (1) of the New York Convention, suggests that the convention should be applied to "…arbitral awards made in the territory of a State other than the State where the recognition and enforcement of such awards are sought....", as well as to "arbitral awards not considered as domestic awards in the State where their recognition and enforcement are sought."

Convention) [Lew J., Mistelis L., Kroll M., 2003: 700], this approach hardly seems compatible with the key purpose of data protection regulation, which is to defend data subjects' rights from possible negative influence by the regulatory environment in the country to which the data is actually transmitted.[80] This purpose has little or no relevance to the seat of arbitration. It should instead entail consideration of the national laws applicable to entities receiving the data (arbitrators, opposing parties, arbitral institution, etc.). In practice this means that the application of data security standards and grounds for data transmission in arbitration may be extremely fragmented.

A second problem with the approach to application of Art. 48 of the GDPR suggested above is that it assumes in effect that the limitations of Art. 48 can always be overridden by the GDPR's other provisions (such as the derogations offered by Art. 49). This is specifically pertinent to arbitration because there are often no international agreements to apply. The presumption would then be that it is always possible to find alternative grounds to justify cross-border data transfer.

That regulatory strategy does not seem very logical because there is no clear reason for imposing a restriction that can be easily ignored by applying another clause of the same regulation. We could perhaps use the "cascade principle" described earlier to settle this problem as well; however, that suggestion does not fully align with the general logic of the GDPR. We can think of several reasons that explain why adequacy decisions take precedence over, say, the derogations that may be available. From the perspective of a regulator, adequacy decisions should be the first recourse because the regulator will have been able to verify the security of data transmission in advance. The data transferring party should also see this approach as acceptable because adequacy decisions release them from complying with the more complex and burdensome requirements of the GDPR. However, neither of these lines of thinking can provide a definitive answer to the question concerning the relationship between Articles 48 and 49 of the GDPR. Until further explanations are provided by the regulatory authorities of the EU, the confusion will continue and leave the transferring party to wrestle with whether they can use other available grounds for the transfer of data (such as those provided by Art. 49) or should instead completely refuse the transfer.

Refusing transfer would be consistent with a more conservative opinion about application of Art. 48. According to that position, Art. 48 may be

[80] See Communication to the EU Parliament.

viewed as restricting reliance on Art. 49(1)(e) of the GDPR only to legal claims pursuant to judgements or decisions which are in turn supported by international bilateral or multilateral agreements.[81] If this interpretation holds (again provided that there are no international agreements that apply to international arbitration), then cross-border data transfer in arbitration would be paralyzed in many ways because the legal claims derogation, which is currently the most suitable ground for transfer of data in international arbitration, would become difficult or almost impossible to apply.

The plain language of Art. 48 of the GDPR also suggests that an international agreement is required in order to *enforce or recognize* a decision or judgment on data transfer to a third country rather than to substitute for or supplement the other grounds for cross-border data transfer provided by the GDPR. As further clarified by Recital 115 of the GDPR, the purpose of this limitation is to preclude extraterritorial application of "laws, regulations and other legal acts" of third countries, which may require data transfer but not provide data protection analogous to that required by the GDPR.[82]

Such a literal interpretation of the GDPR's provisions may suggest a third possibility for applying Art. 48 by maintaining that voluntary compliance with judgements and decisions on data transfer (when no enforcement procedures are involved) falls outside the scope of Art. 48, which would then be applicable only in the event that enforcement of a judgement or decision is required. However, following this interpretation for arbitration proceedings is questionable because even when data transfer is ordered by a tribunal (e.g. as a part of production of evidence), that order has limited potential for enforcement. The main incentive to comply with the order would be to avoid adverse inferences that would be prejudicial to a party that refuses to comply with a disclosure order.

As things currently stand, application of Art. 48 of the GDPR in international arbitration is complicated by a number of factors, including lack of clarity about the exact circumstances in which it should be applied and lack of appropriate international treaties designed for international arbitration as well as the limited enforcement capacity of the tribunals' orders. This

[81] See the report by Ernst & Young. Practical considerations for cross-border discovery under the General Data Protection Regulation (GDPR). Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-e-discovery-practical-considerations-for-cross-border-discovery-under-gdpr.pdf (accessed: 14.04.2021)

[82] Recital 11 of the GDPR.

lack of clarity also brings into question the proper application and pertinence of Art. 49(1)(e) of the GDPR for international arbitration.

Application of the legitimate interest derogation

The last resort for a derogation that permits data transfer in international arbitration when none of the previously described grounds and derogations can be applied is provided by Art. 49(1)§2 of the GDPR (i.e. the legitimate interest derogation).[83] In practice, this provision may be invoked, if not all the data that party is willing to transfer falls under the legal claims derogation (e.g. it may be difficult to establish direct relevance between the data in question and the arbitration proceedings) [Paisley K., 2018: 876].

In order to comply with Art. 49(1)§2 of the GDPR, the disclosing party should ensure compliance with the following conditions:

data transfer is not repetitive;

only a limited number of data subjects is concerned;

data transfer is necessary for the purposes of "compelling legitimate interests pursued by the controller" and such interests "are not overridden by the interests or rights and freedoms of the data subject";

the controller has assessed all the circumstances surrounding the data transfer and has used that assessment to introduce suitable safeguards for protecting personal data.

In addition to compliance with those requirements, a data controller relying on the legitimate interest derogation should also notify the supervisory authority of the transfer.[84]

A comparison of this provision with Art. 49(1)(e) of the GDPR (the legal claims derogation) points up at least two complications peculiar to the legitimate interest derogation: first, the requirement to notify the supervisory authority during international arbitration could involve a breach of confidentiality; and second, there is a higher threshold for the necessity test that transferring party must meet.[85]

In particular, the disclosing party resorting to Art. 49(1)§2 of the GDPR should be able not only to substantiate that the transfer is necessary, but also to demonstrate that this necessity is derived from "compelling legitimate

[83] Guidelines on derogations, p. 14.

[84] See §3 of Art. 49(1) of the GDPR.

[85] Guidelines on derogations, p. 12.

interests". There is no direct answer at the moment about whether transfer of data for the purpose of participating in arbitration should be considered as a compelling legitimate interest or not. But the example suggested by the European Data Protection Board in this matter suggests that, in order to comply with the established standard, the disclosing party should be able to demonstrate that transfer of data was required as a protection "from serious immediate harm or from a severe penalty which would seriously affect…business".[86]

It follows that this ground may be applied in arbitration depending on the factual circumstances in arbitration that frame the cross-border data transfer and on the potential negative consequences incurred by failing to transfer. However, the issue of notification remains a substantial obstacle to ready reliance on this ground because confidentiality is a basic principle of arbitration, as has previously been mentioned.

The foregoing analysis shows that all of the grounds on which a party can rely for justifying cross-border data transfer provide almost no solution that would suit international arbitration. Even resort to the legal claims and legitimate interest derogations does not provide the transferring party with full protection from claims and challenges related to non-compliance or improper compliance with the GDPR requirements; and, equally important, neither of those rules take into account such distinctive features of arbitration as the requirement of confidentiality or the predominantly voluntary nature of arbitration.

Conclusion

International arbitration is now faced with data protection requirements (and in particular the GDPR) that allow nearly no acceptable or risk-free solutions, which would enable parties to meet all of the necessary requirements. This is because the requirements have been formulated without taking into account industry specifics (for our purposes, the specific rules and principles that distinguish international arbitration from other types of procedures for dispute resolution).[87] Therefore, the incentive to comply may be significantly reduced, and diligent compliance may be supplanted by a formalistic exercise.

[86] Ibid., p. 15.

[87] It should be noted that some jurisdictions, e.g. the USA, historically follow "more of a fragmented and sector-specific approach" [Cooper D., Kuner C., 2017: 48]. Nevertheless, expansion of the digital environment and the huge increase in electronic data exchange largely blurs the differences in regulatory approaches.

Although the specific requirements may differ from jurisdiction to jurisdiction, it would be fair to say that regulators increasingly tend to gravitate toward a more stringent rather than a more relaxed approach to data protection (especially in the context of the cross-border data exchange). For instance, Russian regulation (which, along with the Chinese one, is frequently cited as a major antagonist to the GDPR) does not recognize legal claims derogation to legitimate cross-border data transfer and relies primarily on the data subject's consent or adequacy decisions.[88] Some jurisdictions also apply so-called "blocking statutes" that literally prohibit the transfer of data to foreign jurisdictions and apply criminal penalties to it.[89] Instances of data protection regulations that are nuanced and adaptive are very rare, if not completely absent.

As data protection regulations penetrate almost every aspect of life and business, companies covered by those regulations become more inclined to "tick the right boxes" and find the most convenient ways to justify their practices rather than to protect the real interests of data subjects with due consideration of all relevant circumstances. This outcome has strayed far from the initial ideas that prompted data protection regulation and probably neglects the interests of private data subjects themselves.

In order to overcome this problem and to develop regulations which would be helpful in achieving the important task of private data protection, it is necessary to carefully consider all the industries and sectors that may

[88] In accordance with Art. 12 of the Federal Law of the Russian Federation "On personal data" No 152-FZ 27.07.2006, cross-border data transfer is allowed only subject to the following limited set of conditions: the country to which the data is to be transferred provides adequate protection of personal data (such protection may be ensured either by the fact of being signatory to the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, or by being added to a separate list of states with adequate data protections); the data subject has provided his/her written consent; the data transfer is provided for by an international treaty; the data transfer is provided for by the relevant federal laws and is necessary to protect the Constitution, to ensure the country's defense and state security, as well as to ensure the security of the stable and safe functioning of the transport system; the data transfer is required to execute a contract to which the data subject is a party; the data transfer is necessary to protect the data subject's rights and interests.

[89] 00339/09/EN WP 158: Working Document 1/2009 on pre-trial discovery for cross border civil litigation. 11 February 2009, p. 5. See for example, the French Statute № 68-678 of 26 July 1968, modified by the French Statute No 80-538 of 16 July 1980; the Swiss Criminal Code; China State Secrecy Law; Australian Foreign Proceedings (Prohibition of Certain Evidence) Act 1979, etc. (for more details seethe Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts: a practical guide to navigating the competing currents of International Data Privacy and e-Discovery, 2008 Public Comment Version, 2008 the Sedona Conference, pp. 18–20).

be affected by the data protection regulations and make sure that any such regulation is organically embedded into the existing ecosystems without unnecessarily subverting the principles peculiar to each of them. Building an effective defense for privacy should be the primary purpose.

One possible solution that should be considered in order to reduce the current fragmentation (at least in matters of cross-border transfers) would be to arrive at suitable international conventions that would balance the regulatory concerns of different countries and provide all the stakeholders with greater predictability in data protection requirements.

References

Born G. (2021) *International Commercial Arbitration*. 3rd ed. The Hague: Kluwer Law International, 4250 p.

Born G. (2014) *International Commercial Arbitration*. 2nd ed. The Hague: Kluwer Law International, 4000 p.

Burianski M., Reindl M. (2010) Truth or dare? The conflict between e-discovery in international arbitration and German data protection rules. *Schieds VZ: German Arbitration Journal,* no 4, pp. 182–200.

Cohen S. Morril M. (2017) A call to cyberarms: The international arbitrator's duty to avoid digital intrusion. *Fordham International Law Journal*, no 3, pp. 957–1005.

Cooper D., Kuner C. (2017) Data Protection Law and International Dispute Resolution. In: Collected Courses of the Hague Academy of International Law, vol. 382 Leiden/Boston: Hague Academy of International Law, pp. 9–174.

Graham N., Mehta T. (2015) Safe Harbor in a storm: ECJ rules on data transfers to the US. *Practical Law UK*. Articles 3-619-7150. Available at: https://uk.practicallaw.thomsonreuters.com/3-619-7150?contextData=(sc.Default)&transitionType=Default&firstPage=true (accessed: 20.04.2021)

Kuner C. (2013) *Transborder Data Flows and Data Privacy.* Oxford: University Press, 285 p.

Lew J., Mistelis L., Kroll M. (2003) *Comparative International Commercial Arbitration*. The Hague: Kluwer Law International, 953 p.

Lew J. (2006) Achieving the dream: Autonomous arbitration. *Arbitration International,* no 2, pp. 79–204.

Maldoff G. (2016) White Paper, CIPP/US, IAPP Westin Fellow. The risk-based approach in the GDPR: Interpretation and implications. Available at: https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ (accessed: 20.04.2021)

Paisley K. (2018) It's all about the data: The impact of the EU General Data Protection Regulation on international arbitration. *Fordham International Law Journal*, no 4, pp. 854–908.

Pastore J. (2017) Practical approaches to cybersecurity in arbitration. *Fordham International Law Journal*, no 3, pp. 1023–1029.

Rosenthal D. (2019) Complying with the General Data Protection Regulation (GDPR) in international arbitration — Practical guidance. *Association Suisse de l'Arbitrage Bulletin*, no 4, pp. 822–852.

Schwarz E. (2018) Ernst & Young report. Practical considerations for cross-border discovery under the General Data Protection Regulation (GDPR). Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-e-discovery-practical-consideration сц3у смма4ку4 s-for-cross-border-discovery-under-gdpr.pdf (accessed: 20.04.2021)

Smeureanu I. (2011) Confidentiality in International Commercial Arbitration. International Arbitration Law Library. Vol. 22. The Hague: Kluwer Law International, 232 p.

Tschanz P.-Y. (2006) Switzerland: Confidentiality of Swiss Supreme Court review of arbitral awards. Available at: https://www.mondaq.com/Litigation-Mediation-Arbitration/43062/Confidentiality-Of-Swiss-Supreme-Court-Review-Of-Arbitral-Awards (accessed: 20.04.2021)

Warren S., Brandeis L. (1890) The right to privacy. *Harvard Law Review*, no 5, pp. 193–220.

The Issue of State Sovereignty in Cyberspace

Luidmila Terentieva

Associate professor, International Private Law Chair, Kutafin Moscow State Law University. Address: 9 Sadovaya-Kudrinskaya Str., Moscow 123242, Russian Federation. E-mail: terentevamila@mail.ru

Abstract

The author examines a special approach to establishing the sovereignty of the state in relation to cyberspace, the extraterritorial characteristics of which determine the question of the implementation of the territorial supremacy of the state. The author concludes that the understanding of the state's sovereignty in relation to cyberspace lies not in detailing a set of measures in the form of sovereign powers undertaken in this area, but in constructing the boundaries of cyberspace both in relation to the technical component of the network infrastructure that supports the smooth functioning of the Network, and in in relation to the virtual component of cyberspace. To achieve the goal of the study, the author proposed to combine social, technological and subjective approaches, understanding by cyberspace an artificial telecommunication environment for the implementation of public relations controlled by a wide range of subjects (states, intergovernmental organizations, non-governmental organizations, individuals, etc.), the functioning and maintenance of which is carried out by means of software-technical infrastructure in the form of its physical part (telecommunication networks, computers, servers, routers, processors, satellites, etc.) and a virtual part (operating systems, data transmission standards, hardware applications, software, etc.).

Keywords

cyberspace, sovereignty, Internet, software, digital rights, information.

Acknowledgements: The article was prepared thanks to the financial support of the Russian Foundation for Basic Research (RFFI) as a part of the RFFI's project "Internet Law: from a Concept to a Methodology of Regulating Trans-Border Relations" — project No. 18-29-16061; the funding was awarded based on the results of a competitive review of proposals for projects of interdisciplinary basic research (the competition's code is 26-816: "Transformation of Law in an Age of the Development of Digital Technologies").

For citation: Terentieva L.V. (2021) The Issue of State Sovereignty in Cyberspace. *Legal Issues in the Digital Age,* no 2, pp. 49–67.

DOI: 10.17323/2713-2749.2021.2.49.67

Introduction

The rise of a large-scale extraterritorial multi-site space of information and communication has not only positive aspects, such as interactive communication and the infusion of the principles of transparency and openness into the workings of the traditional societal and governmental institutions; it also carries certain risks — for instance, potentially threatening state sovereignty, which is based on such traditional characteristics as power and territory.

Because the vital qualities of the state, as well as the principles of international law, are deeply entrenched in the traditional concepts of territorial geography, the academe has had to address the following questions: is the system rooted in the 1648 Peace of Westphalia sufficiently well equipped to respond to modern challenges of a network society [Bethlehem D., 2014: 9–24].

The development of digital technologies gave rise to the theory of "digital libertarianism," which counterposes sovereignty of cyberspace to state sovereignty [Tulikov A.V., 2016: 235–243]. The difficulties of objectifying cyberspace through physical parameters have given rise to the argument that geographic territoriality in international law is ineffective and borders between states have been weakened [Anselmo E., 2006: 24–31]; [Malakhov V.C., 2007: 218]; [Benyekhlef K., Gelinas F., 2001:7]; [Kobrin S., 1997: 65–77]; that the concept of territory has changed significantly and borders of states do not coincide with borders of regions over which these states exercise authority [Adams J., Albakajai M., 2016: 256–265]; [Matusitz J., 2014: 713–724]; [Streltsov A., 2017: 88–106]; that territorial sovereigns cannot control cyberspace, which should be governed by its own jurisdiction (or several jurisdictions) specially created for the purpose [Johnson D., Post D., 1996]; and that sovereignty is a fiction [Ivanov V., 2009]. Some researchers have also suggested creating a legal system based on self-regulation since sovereigns cannot exercise their authority over cyberspace, which has no borders [Samarin A.A., 2016:13].

As M.N. Marchenko noted, the argument that state sovereignty is "historically exhaustible" and "susceptible to erosion" not only contributes to undermining the centuries-old school of thinking on sovereignty and its role for society and the state but also erodes the entire methodological foundation of the process of acquiring knowledge about the state and law [Marchenko M.N., 2011: 92–93].

Arguably, any stage of society's technological development accompanied by an acceleration of the pace of globalization can present a convenient opportunity to raise the question of possible elimination of sovereignty and a weakening of the power of state institutions. But despite all the radical ideas about the forthcoming end of geography and state borders, the magnitude of development of economic, political, and social relations in cyberspace calls for a discussion about limits of states' legal powers with regard to these relations.

This problem was also broached in President Putin's decree of May 9, 2017, "On the Strategy of Development of Information Society in the Russian Federation for 2017–2030," in which it is noted in §17, that states have to adapt, practically "on the fly," state regulation in the area of information and information technologies in order to set in place international legal mechanisms that would protect states' sovereign right to regulate information space, including in national segments of the Internet[1].

Before proceeding to establish international legal mechanisms for regulating information space, the following question has to be addressed: is the present territorial concept of the state's sovereignty and jurisdiction is essentially exhausted in this space and do we need new approaches partly based on realities of cyberspace. And assessing the territorial principle of sovereignty and jurisdiction, we should look at a combination of extraterritorial information flows rather than at cyberspace's technological infrastructure, which, possessing certain physical parameters as it does, can be localized fairly easily,

There is a truth to the doctrinal argument that ensuring a state's sovereignty in information sphere and developing a global information society are two mutually exclusive objectives because it is difficult for the state to maintain control over its information policies when this state is strongly integrated into global information society [Abdrakhmanov D.V., 2016: 66–72]. This conflict of concepts, however, can not only produce the idea about a weakening of sovereignty in global information space — it can also give rise to a different approach, such as recognizing the need to take additional measures to strengthen the state's control over information space, as well as its information security.

It should be pointed out that as such, globalization, and information and communication flows, cannot affect sovereignty as an international legal

[1] Compendium of Laws of the Russian Federation [Sobranie zakonodatel'stva Rossiyskoy Federatsii]. 2017. No. 20. Article 2901.

principle. If we assume that they can, it would be tantamount to recognizing that sovereignty can be divided or abridged. If we recognize that the mentioned processes lead to an abridgment of sovereignty, it follows, then, that sovereignty consists of structural elements that can be taken away. State sovereignty, meanwhile, is a qualitative, static category: quantitative characteristics, such as size, volume, completeness or incompleteness, are not applicable to it.

Any abridgement of sovereignty as an international legal principle of sovereign equality of states, of supremacy and independence of a government inside the respective country and in relations with other governments can result in an erosion of the concept of sovereignty and put at risk the very existence of the state, because sovereignty can be transferred only in full (as when one state is incorporated into another as a unit of the federation), and not partially. So raising the question of restricting sovereignty when globalizing, integration and information processes are afoot appears inappropriate.

At the same time, taking into consideration the expansion of collective interests of governments and the entire international community at an age of globalization, scholars allow room for restricting the functions of sovereign states or delegating the state's rights inherent in the state's sovereignty as a primary subject of international law, but only when the concerned state voluntarily agrees to it for the purpose of achieving objectives of public importance [Galushko D.V., 2013: 366–374]; [Moiseyev A.A., 2007: 26].

Relying on the concept of transfer of sovereign rights, rather than of sovereignty itself, S.V.Chernichenko concludes that the principle of sovereign equality of states (including respect for state sovereignty) is not an obstacle to globalization [Chernichenko S.V., 2010: 25–31]. Besides, according to M.N.Marchenko, as states coexist and interact with each other working on global and local problems in today's realities, the social role and importance of state sovereignty, far from becoming weaker, only grows [Marchenko M.N., 2011:100].

The fact that states are bound by political, economic, social and other obligations both at home and internationally has an impact not on sovereignty as an international legal principle but on the realization of states' sovereign rights. The principle of sovereign equality of states meanwhile remains firmly in place.

In academic literature the concept of sovereignty is often represented as having different categories: economic, political, taxational, informational, etc. [Shakhmametiev A.A., 2013: 76–81]; [Khavanova I.A., 2013: 41–51];

[Izbulatov Kh.Kh., 2007: 139–141]; [Kirilenko V.P., Alexeyev G.V. 2016: 14–23]. As was noted by O.Ch.Reut, the application of these adjectives to sovereignty is not at odds with the concept of sovereignty and enables us to clarify one or another dimension of the concept [Reut O.Ch., 2007: 115–124]. At the same time, some thinkers suggest an inverse move — applying an indivisible concept of state sovereignty to one or another sphere [Bachilo I.L., 2016: 76–88]; [Talapina E.V., 2018: 60–67]; [Chernichenko S.V., 2010: 25]. S.V.Chernichenko argues that dividing state sovereignty into separate elements is inexpedient because it is difficult to compile an approximate list of types of sovereignty and define each of them [Chernichenko S.V., 2010: 31].

As it appears, such notions as "political sovereignty," "economic sovereignty," "financial sovereignty" are rather abstract, meaning an autonomous, independent political course pursued by a state in one or another sphere. In each of the mentioned areas states are equally self-sustaining and independent.

A special approach can be applied to state's sovereignty in such specific sphere of information and communication space as cyberspace. As in the concepts of political, economic, financial sovereignty, the key here is the category of state sovereignty, denoting an immutable characteristic of the state's supremacy within its national borders and its independence in international affairs. The cardinal difference of sovereignty as applied to cyberspace, however, is the impossibility of reducing its borders to the state's physical borders, which raises the question of the principles of realization of the state's territorial supremacy in relation to this space.

In scholarship, the question of the workings of sovereignty in cyberspace is often raised by researchers of informational sovereignty. The concept of informational sovereignty originated yet before the birth of cyberspace; because of this, informational sovereignty in the scholarship is vested with a broader meaning — it stands for the state's supremacy and independence in shaping and carrying out its information policy, aimed at protecting the state's security in information space, information sphere, information segment [Yefremov A.A., 2017: 201–215]; [Kucheryavyi M. M., 2015: 11].

In some concepts of information sovereignty, spatial limits of sovereignty in information sphere are often represented as spatial limits of the state's supreme power over the respective national segment of telecommunications environment, first of all the Internet [Streltsov A., 2017: 88–106] or as virtual reality, which is cybernetic space [Polikarpov V.S., Polikarpova Ye.V., 2014: 279–284]. Such a view probably stems from equating cy-

berspace to information space and virtual space, an approach applied by some scholars [Vaganov P.A., 2006: 73–89].

In this case the spheres of sovereignty differ greatly in terms of volume, considering that cyberspace is just one of the elements — a significant one, but only one among other elements — of information space, which is quite wide and includes much more than cyberspace alone.

Some scholars also apply a more narrow approach, using it to conceptualize network sovereignty. Thus, some academics point to constitutive properties of network sovereignty such as the state's supreme power to shape and carry out a national policy aimed at controlling and regulating, within the state's territorial borders, operations of social network structures, as well as suppressing, within other nations' borders, activities of network structures aimed at undermining the state's constitutional basis and constitutional security [Sharifov M.S., 2009: 40–44].

This approach is vulnerable to criticism because it is not clear how social network structures can operate in the respective state. Do these researchers mean establishing sovereignty in relation to the network hardware that ensures a smooth functioning of these social network structures or in relation to information posted online on a site with one or another state's domain name?

What is also unclear is what exactly is meant by network structures: social networks, technological infrastructure or something else? It appears more appropriate, therefore, to talk not about sovereignty in relation to social network structures or the technological infrastructures supporting operations thereof but in relation to cyberspace, which includes all of the above-mentioned elements.

Non-Russian scholars argue that it is impossible to establish sovereignty in relation to cyberspace as such although it may be established in relation to an infrastructure situated within the state's territorial borders, as well as in relation to activities connected with this infrastructure, no matter whether it is publicly or privately owned [Schmitt M., 2013: 25].

Considering the territorial nature of state sovereignty and jurisdiction, it appears beyond doubt that a state can establish sovereignty in relation to cyberspace's technical component physically present on the respective state's territory.

Cyberspace, however, is not tantamount to an array of only material objects (computers, servers, routers, optical fiber cables, etc.), nor is it tantamount to a computerized network consisting of a multitude of com-

puterized subnetworks across the globe. In addition to the technological component, cyberspace includes a plethora of immaterial elements, such as information and software[2]. The main function of cyberspace is virtual: creating an interactive environment for a wide range of actors.

It appears more appropriate, therefore, to define sovereignty in cyberspace not only in relation to the technical component of the network infrastructure ensuring the network's smooth functioning but also in relation to the virtual component of cyberspace.

So, it is necessary to offer a definition of cyberspace in which technological and social approaches converge and to explore the relationship between the concepts of information space and cyberspace.

Definition of cyberspace

In Annex 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization (Yekaterinburg, June 16, 2009) "'information space' means a field of activities related to the formation, generation, transformation, transmission, use, storage of information that [has] an impact, among other things[,] on individual and social consciousness, information infrastructure and information itself"[3].

Information infrastructure is defined in Annex I to the Agreement as "a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information"[4].

The definition of information resources in the Agreement is not very good either — the resources are conceptualized through information infrastructure as well as information as such and its flows, rather than as an autonomous concept[5].

Russian law has adopted a technological approach to conceptualizing information space, informed by the current state of information and communications technologies.

[2] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. May 13, 2014. Pp. 8–9. Available at: https://www.nap.edu/read/18749/chapter/3. (accessed: January 12, 2021)

[3] Byulleten' mezhdunarodnykh dogovorov. 2012. No. 1.

[4] Ibid.

[5] Ibid.

Such technological approach is applied in the Russian Presidential decree of May 9, 2017 "On Strategy of Development of Information Society in the Russian Federation for 2017–2030" (hereinafter referred as to the 2017 Presidential decree) — in this document information space is conceptualized as a combination of information resources created by subjects of information sphere, tools by which the subjects interact, the subjects' information systems, and the requisite information infrastructure.

Scholars, too, often apply the technological approach to conceptualizing information space, which they define as a combination of information resources and infrastructural facilities comprising national and cross-border computerized networks, telecommunication systems and public use networks, data bases and data banks, other trans-border information transmission channels [Girich V.L., 2007]; [Kopylov V.A., 2002: 234]; [Prosvirnin Yu.G., 2000: 64].

It is easy to notice that the quoted definitions are somewhat circuitous, with one concept defined through another. Thus, the definition of information space contained in the Presidential decree of May 9, 2017, includes quite a lot of terms that are either authoritatively explained in other regulatory documents or have been doctrinally interpreted in the absence of a definition in law.

Thus, the concept of information system is entrenched in Federal Law 2 "On Information, Informational Technologies, and Protection of Information," adopted in 2006: according to the text of the law, an information system is the combination of information in data bases and information technologies, hardware and software employed to process it[6].

The concept of information resources was contained in §2 of the now repealed Federal Law 24 "On Information, Informatization and Protection of Information" (approved in 1995): the definition included individual documents and individual arrays of documents, as well as documents and arrays of documents in information systems (libraries, archives, funds, data banks, other information systems)[7].Academics categorize information resources as an element of information systems, conceptualizing these resources as a combination of documented information covered by special

[6] Federal Law No. 149-FZ July 27, 2006 On Information, Information Technologies, and Protection of Information // Compendium of Laws of the Russian Federation. 2006. No. 31 (part I). Article 3448.

[7] Federal Law No. 24-FZ February 20, 1995 On Information, Informatization, and Protection of Information // Compendium of Laws of the Russian Federation. 1995. No. 8. Article 609 (now repealed).

rules, as set out in law or other regulatory instruments, with respect to creation and documentation of information items, categories of information included into an information resource, procedures and conditions for provision, usage, dissemination, etc. [Amelin R.V., 2018].

Yet another component of information space — "information infrastructure" — is conceptualized in the 2016 Presidential decree "The Doctrine of Information Security" (hereinafter referred to as the Information Security Doctrine)[8], where it is defined as "a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties signed by the Russian Federation."

It should be noted that the above mentioned definitions, contained in the presidential decrees and federal laws, are somewhat difficult to grasp. For instance, the term "information systems" is in fact referenced twice — first, in the concept of information space presented in the 2017 presidential decree, and second, as an element in the concepts of information infrastructure and information sphere, which are elaborated in the 2016 Information Security Doctrine. Besides, as it references Internet websites, the definition of information infrastructure is practically a carbon copy of the definition of information resources from the definition of information space, because websites can be categorized as arrays of documents in information systems.

At the same time, the above concept of information infrastructure in the context of cyberspace highlights the combination of material and non-material infrastructures of cyberspace, which include material equipment, such as communication networks and informatization objects (telecomunication networks, servers, routers, processors, satellites, cables, etc.), and non-material assets, such as information resources and websites.

S.A. Dementiev is right arguing that when information space is approached only in terms of technology, such approach emphasizes only a method for achieving information space and the information person, ignoring the substance of such space and such person [Dementiev S.A., 2017: 145–149].

In the humanities it is barely possibly, and hardly necessary, to formulate concepts of information space through an exhaustive description of technological characteristics referenced therein. Formulating the respec-

[8] Decree of the President of Russian Federation of December 5, 2016. No. 646. // Compendium of Laws of the Russian Federation. 2016. No. 50. Article 7074.

tive concepts, one should rather use a non-deterministic approach reflecting these concepts' substantive characteristics (communicativeness, decentralization, extraterritoriality, etc.).

It follows from the above that information space should be conceptualized as an environment where information is created, relayed, consumed and used, without an emphasis on channels by which it is transmitted and received. Technologies are undoubtedly one of the key factors in information space's functioning. It is worth noting though that, firstly, when a particular period's technological context is ignored, the argument about the absence of information space at that period appears futile. Secondly, law influences not methods by which technological infrastructures are formed but results of these infrastructures' impact.

The definition at issue should be centered on the environment in which social interactions, governed by law, occur, whereas organizational and technical aspects of information space should be referenced in the definition only inasmuch as they reflect the manner in which the respective environment is formed.

Considering that the specifics of cyberspace are conditioned by its technological characteristics, the academic community has to provide a definition of cyberspace that would reflect a combination of its technical, social, and institutional elements.

The technology-oriented definitions of cyberspace emphasize technological infrastructures, and arrays of methods used to store, change, and utilize information.

In National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) 2008 cyberspace is defined as "the independent network of information technology infrastructures, [which] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"[9].

In the U.S. Department of Defense's National Military Strategy for Cyberspace Operations (p.3), cyberspace is defined as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[10]

[9] Available at: https://fas.org/irp/offdocs/nspd/nspd-54.pdf (accessed: January 25, 2021)

[10] Available at: https: hsdl.org (accessed: January 25, 2021)

The Western scholarship has provided definitions of cyberspace as "a domain characterized by the use of computers and other electronic devices to store, modify, and exchange data via networked systems and associated physical infrastructures." [Schaap A. , 2009: 126].

Another definition of cyberspace is that of "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures." Some researchers came up with a social definition of cyberspace, probably taking into consideration the word's etymology — it consists of two elements, first, "cyber," originating from the Greek word *kybernao/kybernan*, meaning "to govern," "to control," [Kuehl D., 2009] and "space".

Social scientists and philosophers define cyberspace as a socio-cultural factor having an impact on development of the network society [Khutornoi S.N., 2003: 9–10]. Sometimes cyberspace is defined through a metaphorical abstraction, used for describing objects typical for computer networks — for instance, a website is described as located in cyberspace and network communication, as "communication in cyberspace." [Baryshev R.A., 2009: 9–10]; [Volov A.G., 2011: 49–54].

Identifying characteristics of cyberspace, scholars usually refer to this space's indivisibility, the fact that it cannot be reduced to borders of a physical space [Voinikanis Ye.A., 2013], fluidity and variability of cyberspace's borders [Dobrinskaya D. Ye., 2018: 52-70], geographic indeterminacy, a trans-border character [Fedotov M.A., 2016: 164-182], multidimensionality, and the absence of linearity, length, physical parameters [Anselmo E., 2006: 25]. Theoreticians also point to continuous variability of cyberspace's structure — the result of birth and death of information resources, changes in the directions of information flows, and creation of new technologies of processing and transmitting information [Bondarenko S.V., 2002: 61–64].

What makes cyberspace unique and distinctive is its global character — its universal accessibility and trans-border nature, allowing unlimited numbers of users to interact across national borders.

M.S. Dashyan approaches cyberspace as a social domain, identifying some of its essential properties, such as convergence (a mixture of traditional phenomenons and processes within one open system — the Internet); a hierarchical order, decentralization, extraterritoriality (the Internet forms a new information space — cyberspace, outside the limits of real world, so it cannot be measured with physical and chemical measuring tools); a democratic character [Dashyan M.S., 2007].

At the same time, some researchers argue that defining cyberspace is a difficult task [Hitsevich N., 2015: 16], which probably explains the emergence of somewhat fanciful descriptions of it — for instance, an electronic nervous system of our society that lends a dynamic structure to cyberspace [Manuel C., 2003: 36]. An academic inquiry into cyberspace through the lens of engineering and social scientists produced, in Russia and elsewhere, bipartite and tripartite definitions of cyberspace. Thus, cyberspace is explored both as a physical entity and a virtual one. "The physical part is the millions of networked information and communication technologies that create and enable it: computers, servers, routers, processors, satellites, switches, and cables. The virtual part is formed by electronic connections and by the data sent between and stored in the pieces of its physical infrastructure." [Spade C., 2012: 6]. Changes in cyberspace are caused by changes in, and development of, new hardware and software.

D. Clemente in his study identifies already three layers of cyberspace: "the physical layer (i.e. hardware such as submarine and ethernet cables, routers and switching devices), the logical layer (i.e. software or lines of code that allows the hardware to function and communicate), and the social layer (i.e. interaction between online personas that represent people or, increasingly, machines)." [Clemente D., 2013: 5].

There can be little doubt that cyberspace's main function is embedded in virtual reality — it consists in providing an environment where users across the globe can interact. And this function is activated by physical elements (telecommunication networks, computer systems, servers, routers, processors, satellites, switchboards, and cables) and non-physical elements (applications, software, etc.) of cyberspace alike.

The communicative and technological properties of cyberspace are reflected in the international standard ISO/IEC 27032: 2012 Information technology Security techniques. Guidelines-for cybersecurity, issued by the International Organization for Standardization (ISO) (hereinafter referred to as ISO/IEC 27032: 2012). In the document's §4.21 cyberspace is defined as "a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks."[11]

[11] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed: March 23, 2021)

Cyberspace, therefore, can be regarded both as a virtual communications environment and as certain electronic carriers providing access to this environment.

In Russian scholarship, likewise, two approaches to cyberspace — technological and social — coexist [Vagin O.A., Goriainov K.K. et al, 2018].

In the technological theoretical framework, cyberspace is an information and telecommunication instrument for transmitting, processing and storing information (principles of organization of hardware networked environment, selection of networking protocols, organization of address spaces, etc.). From the vantage point of social sciences, cyberspace is a complex socio-cultural phenomenon that influences many facets of society's life and forms a special environment in which certain types of activity and specific social relations occur[12].

Defining cyberspace, one should take into consideration subject-oriented approach as well. Management of cyberspace consists in coordinating the processes of distribution of address spaces, exploitation of root servers, creating and administering systems of domain names and internet addresses, etc. Managers of cyberspace include not only national governments and intergovernmental organizations, but also certain national and international non-governmental organizations: Internet Society (ISOC), Internet Corporation for Assigned Names and Numbers (ICANN), etc., as well as open communities, such as Internet Engineering Task Force (IETF). The Working Group of Internet Governance (WGIG) at its meetings in 2004–2005, too, referenced a large group of entities managing the Internet: governments, private businesses, civic society, intergovernmental and non-governmental international organizations, as well as other forums[13].

It is this type of management by a large group of stakeholders (governments, non-governmental organizations, private persons, etc.) that defines certain features of cyberspace, which, unlike terrestrial, aerial, cosmic and marine spaces, that is the realms traditionally governed by international law, does not have a "natural" origin and is a product of human creativity. Cyberspace is an artificial environment for creating, transmitting and using information.

[12] Ibid.

[13] Background Report. World Summit on the Information Society. Available at: http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf (accessed: January 20, 2019)

Conclusion

So, defining cyberspace, one should take into account not only its technological and social elements, but also its subject-oriented component.

It should be noted that although the above mentioned 2017 Presidential decree provides definitions of such modern phenomena as internet of things, cloud computing, big data processing, etc., it does not contain a definition of cyberspace. As for international documents, the term "cyberspace," without a definition, comes up in the 2000 Okinawa Charter on Global Information Society[14] and the 2001 Convention on Cybercrime[15].

Although the Russian legislation does not have a definition of cyberspace, attempts to conceptualize it were made by the authors of the Draft of the Concept of Cybersecurity Strategy in the Russian Federation[16]. In the Draft cyberspace is a particular element of information space with clear boundaries, and also a type of operations in information space, which are brought about by a combination of communication channels of the Internet and other telecommunication networks, technological infrastructure enabling their functioning, and all forms of human activities (by individuals, organizations, governments) carried out via them.

The definition of cyberspace in the 2016 Information Security Doctrine, too, stresses technological characteristics, defining cyberspace as information systems and sites in the information and telecommunications system Internet. "The Internet" and "cyberspace," however, are not synonymous. The Internet is just one type of computer networks among others.

Cyberspace includes, but is not limited to, the Internet. Technology-wise, cyberspace includes computers that can be either plugged into or unplugged from the Internet, as well as networks, which can or cannot be a part of the Internet[17].

As was noted by Yu. V. Anokhin and M. P. Baranov, a computer unplugged from the Internet can process information and create a virtual space for a user working on it, while also influencing this user's mind. They add that activating a software — for instance, a computer game — users

[14] Okinawa Charter on Global Information Society, July 22, 2000. Diplomaticheskiy vestnik. 2000, no 8, p. 52.

[15] The Convention came into force on July 1, 2004. The Russian Federation is not party to it.

[16] Available at: URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed: February 21, 2020)

[17] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues…

enter in an indirect relationship with this game's creators, falling under the sway of images and symbols programmed by the creators [Anokhin Yu.V., Baranov M.P., 2019: 14–24].

Because cyberspace comprises ordinary in-house computer networks ("extranets"), as well as virtual networks connecting private networks of different companies ("intranets"), one can definitely conclude that cyberspace as an idea is broader than the "Internet network." And considering that cyberspace includes a wide range of communication networks, it is precisely the notion of cyberspace that should be employed determining what state should have jurisdiction over a matter.

ISO/IEC 27032: 2012, defining cyberspace as "a complex environment resulting from the interaction of people, …supported by …communications technology," conceptualizes the Internet, in §4.29, in a more technological vein, as "a global system of inter-connected networks in the public domain"[18].

Cyberspace thus is one of the elements of information space, which is an environment of social interactions whose functioning is supported by a combination of telecommunication networks and by a technological infrastructure. And social interactions among different subjects of law can be carried out without a connection to the geographic territory of a particular state.

If we are to converge social, technological and subject-oriented approaches, here is what appears to be the most apt definition of cyberspace: an artificial telecommunications environment in which social interactions occur, which is managed by a wide range of subjects of private and public law, and the functioning and maintenance of which are carried out via the software-and-hardware infrastructure consisting of material elements (telecommunication networks, computers, servers, routers, satellites, etc.) and non-material elements (software, data transfer standards, applications, software, etc.).

References

Abdrakhmanov D.V. (2016) State sovereignty and information society: mutual connection and mutual dependence. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta,* no 4, pp. 66–72 (in Russian)_

[18] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed: March 23, 2021)

Adams J., Albakajai M. (2016) Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, no 6, pp. 256–265.

Amelin R.V. (2018) Federal and Municipal Information Systems in the Russian Information Legislation: A Theoretical Legal Analysis. Garant.ru (in Russian)

Anokhin Yu.V., Baranov M.P. (2019) Doctrinal characteristic of the ideological function of the state in virtual space. *Zhurnal rossiyskogo prava*, no 8, pp. 14–24 (in Russian)

Anselmo E. (2006) Cyberspace in international law: does the rise of the Internet give the lie to the territorial principle in international law? *Ekonomicheskie strategii*, no 2, pp. 24–31 (in Russian)

Bachilo I.L. (2016) Conceptual framework of information law and the information security system. *Trudy Instituta gosudarstva i prava RAN,* no 3, pp. 76–88 (in Russian)

Baryshev R.A. (2009) Cyberspace and Alienation. Candidate of Philosophical Sciences Summary. Moscow, pp. 9–10 (in Russian)

Benyekhlef K., Gelinas F. (2001) The International Experience in regard to Procedures for Settling Conflicts relating to Copyright in the Digital Environment. *UNESCO Copyright Bulletin*, no 4, pp. 3–19.

Bethlehem D. (2014) The End of Geography: The Changing Nature of the International System and the Challenge to International Law. *European Journal of International Law*, no 1, pp. 9–24.

Bondarenko S.V. (2002) Social community of cyberspace. *Informationnoye obschestvo*, no 4, pp. 61–64 (in Russian)

Chernichenko S.V. (2010) Is state sovereignty divisible? *Yevraziyskiy yuridicheskiy zhurnal*, no 12, pp. 25–31 (in Russian)

Clemente D. (2013) Cyber Security and Global Interdependence: What Is Critical? Available at: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf (accessed: February 21, 2020)

Dashyan M.S. (2007) Law of Information Highways: Legal Regulation of the Internet In: Pravo informatsionnykh magistraley: voprosy pravovogo regulirovaniya v sfere Internet. Garant.ru. (in Russian)

Dementiev S.A. (2017) Transdisciplinary analysis of information space of modern society. *Vestnik Krasnodarskogo universiteta MVD Rossii,* no 4, pp. 145–149 (in Russian)

Dobrinskaya D.Ye. (2018) Cyberspace: a territory of modern life. *Vestnik Moskovskogo universiteta*, no 1, pp. 52–70 (in Russian)

Fedotov M.A. (2016) Constitutional responses to challenges of cyberspace. *Lex Russica*, no 3, pp. 164-182 (in Russian)

Galushko D.V. (2013) State sovereignty in international law. *Vestnik Voronezhskogo universiteta*, no 1, pp. 366–374 (in Russian)

Girich V.L., Chuprina V.N. (2007) Global information space and access to the world's resources. Available at: URL: http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf. (in Russian)

Hitsevich N. (2015) Intellectual property rights infringement on the Internet: an analysis of the private international implications. Available at: http://openaccess.city.ac.uk/17914/ (accessed: November 1, 2020)

Ivanov V. (2009) The state and sovereignty. A discussion of sovereignty. Available at: URL: http://www.russ.ru/Mirovaya-povestka/Gosudarstvo-i-suverenitet (accessed: May 10, 2020) (in Russian)

Izbulatov K.K. (2007) Methodological tools for political and legal inquiry into the notion of economic sovereignty. *Filosofiya prava*, no 3, pp. 139–141 (in Russian)

Johnson D., Post D. (1996) Law And Borders: The Rise of Law in Cyberspace. Available at: https://cyber.harvard.edu/is02/readings/johnson-post.html (accessed: May 10, 2020)

Kopylov V.A. (2002) *Information Law*. Moscow: Delo, 512 p. (in Russian)

Khavanova I.A. (2013) Fiscal (taxation) sovereignty and its limits in integrationist alliances. *Zhurnal rossiyskogo prava*, no 11, pp. 41–51 (in Russian)

Khutornoi S.N. (2003) Cyberspace and the Formation of Network Society. Candidate of Philosophical Sciences Thesis. Voronezh, 166 p. (in Russian)

Kirilenko V.P., Alexeyev G.V. (2016) State sovereignty in the present-day geopolitical situation. *Upravlencheskoe konsul'tirovanie*, no 3, pp. 14–23 (in Russian)

Kobrin S. (1997) Electronic cash and the end of national markets. *Global Issues*, vol. 2, pp. 65–77.

Kucheryavyi M.M. (2015) The Russian state's policies of information sovereignty in the modern globalized environment. *Upravlencheskoe konsul'tirovanie*, no 2, pp. 8–15 (in Russian)

Kuehl D. (2009) From Cyberspace to Cyberpower: Defining the Problem» in Cyberpower and National Security 48. Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210 (accessed: February 15, 2021)

Malakhov V.C. (2007) *The State in an Age of Globalization.* Moscow: Knizhny dom, 252 p. (in Russian)

Manuel C. (2003) *The Internet Galaxy: Reflections on the Internet, Business and Society.* Oxford: University Press, 292 p.

Marchenko M.N. (2011) *The State and Law in an Age of Globalization.* Moscow: Prospect, 656 p. (in Russian)

Matusitz J. (2014) Intercultural perspectives on cyberspace: An updated examination. *Journal of Human Behaviour in the Social Environment,* vol. 24, pp. 713–724.

Moiseyev A.A. (2007) Relationship Between Sovereignty and Supranationality in the Modern International Context of Globalization. Doctor of Juridical Sciences Summary. Moscow, 45 p.

Polikarpov V.S., Polikarpova Ye.V. (2014) The newest information and communications technologies and Russia's information sovereignty. *Informatsionnoe protivodeystvie ugrozam terrorizma,* no 23, pp. 279–284 (in Russian)

Prosvirnin Yu. G. (2000) *Information Law*. Voronezh: University, p.64 (in Russian)

Reut O.Ch. (2007) Adjectives of sovereignty. Sovereignty as an adjective. *Polis*, no 3, pp. 115–124 (in Russian)

Samarin A.A. (2016) Extraterritorial Effects of Law. Candidate of Juridical Sciences Summary. Nizhny Novgorod, 31 p. (in Russian)

Schaap A. (2009) Cyber Warfare Operations: Development and Use under International Law. *Air Force Law Review*, vol. 64, pp.121–173.

Shakhmametiev A.A. (2013) Taxation sovereignty and taxation jurisdiction of the state. *Sovremennoe pravo*, no 3, pp. 76–81 (in Russian)

Sharifov M.S. (2009) Sovereign power in cyberspace and in network space. *Sovremennoe pravo*, no 6, pp. 40–44 (in Russian)

Schmitt M. (2013) *Tallinn Manual of the International Law Applicable to Cyber Warfare.* Cambridge: University Press, 215 p.

Spade C. (2012) Information as Power: China's Cyber Power and America's National Security. Available at: https://itlaw.wikia.org/wiki/Information_as_Power:_China%27s_Cyber_Power_and_America%27s_National_Security (accessed: January 12, 2021)

Streltsov A. (2017) Sovereignty and jurisdiction of the state in an age of information and communication technologies in the context of international security. *Mezhdunarodnaya zhizn*, no 2, pp. 88–106 (in Russian)

Talapina E.V. (2018) State sovereignty and information space: new objectives of law. *Gosudarstvo i pravo*, no 5, pp. 60–67 (in Russian)

Tulikov A.V. (2016) International legal thought in an age of the development of information technologies. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*, no 3, pp. 235–243 (in Russian)

Vaganov P.A. (2006) Legal defense of cyberspace in the United States. *Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie, n*o 4, pp. 73–89 (n Russian)

Vagin O.A., Goriainov K.K. et al (2018) *Theoretical Framework of Crime Detection and Investigation.* Garant.ru. (in Russian)

Voinikanis Ye.A. (2013) Intellectual Property Law in a Digital Age: A Paradigm of Balance and Flexibility. Garant.ru. (in Russian)

Volov A.G. (2011) Philosophical analysis of the idea of "cyberspace". *Filosofskie problemy informatsionnykh tekhnologiy i kiberprostranstva, n*o 2, pp. 49–54 (in Russian)

Yefremov A.A. (2017) Formation of the concept of information sovereignty of the state. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 201–215 (in Russian)

Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace

Shubh Gupta

PhD Scholar, Centre for Studies in Science Policy, Jawaharlal Nehru University. Address: 212 Chandrabhaga Hostel, Jawaharlal Nehru University, New Mehrauli Road 110067, New Delhi, India. E-mail: Shubhgupta008 @gmail.com

Reeta Sony A.L.

Assistant Professor, Centre for Studies in Science Policy, Jawaharlal Nehru University. Address: Warden Flat N0. 4, Godavari Hostel, Jawaharlal Nehru University, New Mehrauli Road 110067, New Delhi, India. E-mail: reetasony@mail.jnu.ac.in

Abstract

The dawn of the neocolonial project has seen the emergence of a new space: data. Data is a raw material that can be stitched, processed and marketed in the same way as the East India Company (EIC) used to do with India's cotton. EIC, which started as one of the world's first joint-stock companies, turned into a wild beast, building a corporate lobby with the help of lawyers and MP shareholders to amend legislation in its favor. The EIC became a particularly atrocious and innovative colonial project that directly or indirectly controlled continents, thanks to an army larger than the army of any nation-state at the time. The Drain Theory of Dadabhai Naroji have opened India's eyes to how the EIC was taking raw material from the country and converting it into a finished product that was marketed in India again in the same way as raw data is being processed outside India and then marketed here today. In today's digital era, big corporations need not own big armies, as companies are protected by nation-states and bailed out when required. Today, one does not need to travel overseas to explore and conquer Gold, God and Glory; instead, they are a click away. The neocolonial project runs on digital platforms, while the popular narrative of bridging the digital divide and giving internet access to millions of people resembles the idea of the "white savior" liberating the "noble savage" through modern Western education. Facebook's grand plan of providing free internet to all can be best understood as a neocolonial strategy to mine the data of billions by equating it with water and land. Similarly, the Cambridge Analytica scandal provides an example of how neocolonial forces can influence the fundamental democratic process of electing a government. Therefore, nations endorsing democratic values should be especially wary of the trap of neocolonialist forces, as such nations are particularly vulnerable to their project. This paper critically study the cyber security infrastructure and policies in India and analyze the India's approach towards cyber sovereignty and data colonialism and thereafter examine the India's strategic position in cyberspace and suggest policy recommendations.

Keywords

data colonialism; cyber sovereignty; data sovereignty; cyber strategy; India's cyber strategy; India's data policy.

For citation: Gupta S., Sony R.A.L. (2021) Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace. *Legal Issues in the Digital Age,* no 2, pp. 68–81.

DOI: 10.17323/2713-2749.2021.2.68.81

Introduction

Neocolonialists view "data" as a raw material that can be stitched, processed and marketed in the same way as the East India Company once did with India's cotton. India supplied raw cotton to British mills that processed it into a finished product and resold it to British colonies [Brain J., 2021]. Britain was able to mass-produce cotton products thanks to rapid technological progress and gain a monopoly on the textile industry with the help of its imperialist policies. The finished product was much cheaper than existing products at the time and created a fashion that led the colonized to "mimic"[1] the colonialists. Even after the British physically departed from India in 1947, they left it with a colonized mindset thanks to different institutions they had created during their tyrannical rule [Preeti, 2016].

Edward Said's [2003: 1–28, 350–353] *Orientalism* shaped the discourse on post-colonialism and provided an alternative to orientalist cultural studies. Said defines orientalism as "a relationship of power, of cultural domination, the cultural equivalent of the colonialism which it accompanied" (Young R., 1995). We experience and access the power of data using the narrative perpetuated by techno-orientalists, who want to maintain the old power relationship and convert it into economic value. We have to understand that Said's work did not criticize Western knowledge; rather, it denounced the power relationships inscribed in this knowledge. Along the same lines, this chapter attempts to explore how data is seen from an Asian perspective, the power relationships it entails, and the major actors in these relationships.

The former CACI International employee Clive Humby coined the motto "*data is new oil*" (Haupt M., 2016). This narrative was pushed worldwide

[1] Bhabha H. (1984) describes how the colonial mimicry becomes a desirable trait for the colonized. For further information please refer to the citation.

to make us believe that data is like an exhaustible natural resource that will help us fuel our economy. Later, when colonized entities began to realize that, if data is indeed like oil, sovereign nations should not let tech giants extract it for free, Google introduced a new narrative that stated that "*data is more like sunlight than oil*" [Ghosh S., Kanter J., 2019]. Google wants us to believe that, like sunlight, data is a never-ending, ownerless and unperishable product that can be harvested for the improvement of humanity. As we see, whenever a nation tries to regulate its data or the internet in general, a new motto appears to make it return to the order of data colonialism.

Data, however, is neither oil nor sunlight; rather, it is a social construct or cultural object that is "embedded and integrated within a social system whose logic, rules and explicit functioning work to determine the new conditions of possibilities of users' lives" [Cheney-Lippold J., 2011: 164–181]; [Gitelman L., 2013]; [Scholz L., 2018] a specific moment in history. Data preserves and extracts individuals' social lives, turning them into inputs for an economic system that has the potential to shape our habits and practices [Dijck J., 2014: 197-208] . Thus, data has become a new means of exercising power. It is therefore important to know who possesses it.

To counter the ideology of data colonialism propagated by IT companies subtly backed by the U.S., China is pushing the opposite notion of absolute cyber sovereignty which goes against the idea of free and open internet and instead promotes its use as a tool to censor the voice of the common people [Sherman J., 2019a]. China is not the only nation to try to employ massive surveillance tools to monitor its citizen's activities online. Every country is trying to keep an eye on its citizens in one way or another, be it U.K's Karma Police [Brandom R., 2015]. India's Central Monitoring System initiated in 2013, or lawful interception and monitoring systems (LMS) [Singh S., 2013]. While every such surveillance program is run under the garb of national security, what matters is how this data is used by a sovereign nation to exercise control over its citizens and other nations.

The question then arises: which way will India choose? As of today, India is pursuing a strategy of remaining unaligned with any group and taking a flexible stance so as to assure its own interests. Nevertheless, it has the potential to serve as a model for other developing countries and conform its position as a "Vishwa Guru."[2] India can take the Gandhian approach,

[2] Vishwa Guru can be roughly translated as World's Guru(Teacher). India wants to take a role of global leadership in knowledge space based on its ancient knowledge system. Available at: https://www.dailypioneer.com/2019/columnists/the-dream-of-a-vishwa-guru.html (accessed: 03.01.2021)

making everyone learn to spin charkha and become "atmanirbhar" [Bhargava K., 2020], or it can fray its own way, as Dattopant Thengadi suggested in his book *The Third Way*, arguing that India should become neither capitalist nor socialist but rather develop its own code [Thengadi D., 1998]. India has refrained from taking extreme sides, be it in international politics or domestic economics. The rich culture of India has led it to become a mixed economy in which the interests of no person, be it a businessman or the man in the street, receive priority.

1. India's Negotiation in Cyber Space

The Indian Constitution complies with the Universal Declaration of Human Rights by guaranteeing fundamental rights to its citizens and protecting them from discrimination. It secures its citizens from border threats by other nations, guarantees food and education, protects from financial fraud, etc. Society, culture, and technology change with the passage of time, and law must adapt to these changes so that the rights guaranteed by the constitution remain intact; whenever a new artifact appears in society, it tries to influence the existing order by making institutions either adapt it or change themselves [Jasanoff S., 2004: 13–43]; [Latour B., 1987].

The exponential changes in internet technologies and the penetration of cyberspace into everyone's lifeworld [Ho W.-C., 2008: 323–342] has made governments deal with them directly rather than leaving them exclusively to scientists and technologists. Ever since Edward Snowden revealed the surveillance programs run by America's National Security Agency, the threat of the misuse of cyberspace has been felt in every nook and corner of the world, leading to a growing demand for the just and fair governance of cyberspace. This has led countries like China and Russia to reframe the idea of cyberspace and call for cyber sovereignty. The Chinese-Russian and US models are two different sides of the same coin. Instead of gravitating towards such extremes, developing countries should find a middle path that would allow their citizens to enjoy sovereignty in cyberspace [Sherman J., 2019]. In particular, India should be cautious of US tech companies that are tenaciously pushing their colonial projects in the garb of free access to their platforms. These companies use their platforms to collect raw data from users and then process and synthesize them for their benefits. In this way, public collaboration and interaction is turned into private profit. Further, these companies influence the way users connect with each other and design their platforms in a such way as to shape the social order [Dijck J. et al., 2018]. The new IT rules that try to make social intermediaries more

accountable and responsible reflect India's striving to protect individual rights and provide a just and fair environment for tech companies.

Moreover, democratic countries such as India should refrain from following the path of China, which strives for absolute cyber sovereignty. This approach allows China to exercise control over domestic politics by keeping its citizens and almost all multilateral organizations and forums under constant surveillance. China has imposed its views on developing countries, and these initiatives are being further promoted with the help of the Belt and Road Initiative (BRI) and other tools of Chinese commercial diplomacy as well as Chinese tech firms.

With 503 million internet users and the penetration of the internet into rural India due to falling prices, India ranks second in the world in data consumption [Roser M., 2018]; [Mishra D., Chanchani M., 2020]. As one of the world's top data generators, India has understood the importance of cybersecurity, leading its government to elaborate a cybersecurity policy in 2013. India has become one of the leading spokesmen for Asian and African countries on world platforms on representing and safeguarding rights to create, consume and process data. A personal data protection bill was introduced in India in 2019 to safeguard the processing of the key data of individuals; however, the final law is still being drafted. However, the country should not be lax about our cybersecurity front, as there have been repeated cyberattacks on the Indian cyber infrastructure: recently, the cybersecurity of the Kundakulam Nuclear Power Plant was breached [Madhavan N., 2019].

Having one of the highest numbers of internet users, India should urgently adopt comprehensive policies that would allow to bring any Indian or foreigner malefactor to justice. India needs to think of building its own cybersecurity infrastructure and cybersecurity policies and keep a constant watch whether it is not taking any extreme step of cyber sovereignty or data colonialism, as India plays a major role in shaping the behavior of other developing countries.

2. Understanding the importance of cyberspace in the context of national security

Let us begin by discussing why cyberspace is called "cyberspace" and not a "cyber system" or "cyber field."

In his "global cultural flows" model, A. Appadurai [Apparadurai A., 1991] defines five categories of global processes: technospace, finance space, media space, ideospace and ethnospace. These spaces are not lim-

ited by regional or national boundaries: there are multiple actors who act as nodes in a network whose flow depends on cultural practice. So, every space has its associated culture. While space is usually seen as an abstract entity or a mere receptacle of human actions [Kokot W., 2007: 10–23]. On contrary "Cultural spatiality"[3] theory treats space as a conceptualization of cultural models and a medium and product of social practice.

The space where internet operates was first called "cyberspace" in science fiction. Later, there arose the debate whether cyberspace is a social construct or an extension or evolution of existing space. It was widely accepted that cyberspace refers not to an abstract space but to a space where multiple interactions take place, leading to the definition "Cyberspace is relative, mutable, and constituted via the interactions among practice, conceptualization, and representation" [Cohen J., 2007].

When we view cyberspace as a real space, a new regulatory challenge emerges: who will regulate this space and how. The evolution of the network space is disrupting the existing nation-state conception of sovereignty.

One school of thought considers cyberspace to be a global common such as air or river and sea water. However, if it is a global common, what international laws apply to it? Who shall be responsible in the case of cyberattacks on a nation's cyberspace? Unlike natural global commons, cyberspace is a man-made common that enables the flow of data and information without barriers. If we try to constrain it within national boundaries, it will become intranet rather than internet. At the same time, critical infrastructures such as banking and defense remain within national boundaries while attacks can come from anywhere in the world, as cyberspace is borderless. Therefore, it is important to frame global laws and regulations that can help to facilitate the free flow of information.

After Edward Snowden's disclosures,[4] many developed and developing countries began to show concern about the spying taking place on the internet and its effects on their national security. A widespread demand voiced by the Chinese media was to restrict American Internet firms from the Chinese domestic market so as to protect Chinese infrastructure from

[3] Cultural spatiality theory was proposed by Hauser — Schäublin and Dickhardt in their volume "Kulturelle Räume — räumliche Kultur" [Hauser-Schäublin & Dickhardt, 2003].

[4] The National Security Agency (NSA) of United States was running a massive surveillance program codenamed PRISM, which accessed the data of leading US companies and official representatives of other sovereign Nations. The PRISM's agendas were disclosed by Edward Snowden in June 2013.

subversion [Lindsay J., 2015]. At the same time, a US Congressman charged China with establishing cyberwar rooms from which it could hurl digital bombs at other countries. There is a lot of contention in this space. Therefore, it is very important for India to think about its national interests and act more flexibly so as to facilitate its own industry rather than serving as a mere market of internet users.

3. The debate around cyber sovereignty and data colonialism

Lu Wei, then head of China's State Internet Information Office and subsequently the director of the Cyberspace Administration of China (CAC), said at the Second China–South Korea Internet Roundtable that, just as national sovereignty had been extended to seas and oceans in the 17th century and air space in the 20th century, so it will further extend to cyberspace in the 21st century [Segal A., 2020: 85–100]. Lu firmly stated that "cyberspace cannot live without sovereignty." This clearly defined China's position in cyberspace. China is propagating the idea of cyber sovereignty with all its might. This idea helps China to exercise control over its domestic politics through the constant surveillance of its citizens. China also has tremendous influence on multilateral organizations and forums as well as on developing counties with the help of its Belt and Road Initiative (BRI). At the same time, state-of-the-art Chinese tech firms and other tools of commercial diplomacy are acting as catalysts in promoting the idea of cyber sovereignty.

In short, cybersecurity has become a national priority of China, which envisages to become a cyber power by actively shaping the global internet narrative. At the 2015 World Internet Conference in Wuzhen, President of the People's Republic of China Xi Jinping said "cyber sovereignty means respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet and to equal participation in international cyberspace governance. He argued that states should refrain from engaging in cyber hegemony, interfering in other countries' internal affairs, and engaging in, tolerating, or supporting online activities harming the national security of other countries". [Xi Jinping H.E., 2015]. As China is aware of its dependence on US technology firms, it is imposing restrictions on the latter in order to protect its cyber sovereignty and to develop its own firms. In September 2014, the China Banking Regulatory Commission called for 75% of ICT products used in banks to be controlled and secured by 2019 [Segal A., 2016]. The document further stated that every bank has to submit secure codes to the

Chinese government, which means creating a backdoor in all hardware and software. This was interpreted by international firms as an attempt to throw them out of the Chinese market [Mozur P., 2015].

In February 2019, the Russian Federal Assembly (Parliament) have approved the Digital Sovereignty Bill to nationalize the country's internet known as "Runet". Runet requires a separate Domain Name System (DNS), countering the hegemony of the US-backed global non-profit organization ICANN that controls global Internet DNS allocation. This will allow Russia to build an agile system that provides protection from various cyberattacks. Further, the new law also includes cross-border mobile and satellite connections in order to maintain the integrity of the network along with a system for closely monitoring all kinds of international connections and filtering them, if found suspicious. However, this law has raised numerous questions, and a large number of people have gone into the streets to protest against its limitation of internet freedom; many other people have complained about the additional control and monitoring of their internet activities. Internet access is provided only through government-licensed service providers. These providers must permit IP blocking, DNS hijacking, keyword inspection, etc. Both China and Russia have described such an approach as being effective and efficient for furthering national security and economic well-being [Venables A., 2019].

In 2017, a statement by BRICS (Brazil, Russia, India, China, and South Africa) highlighted cyber sovereignty as a key principle of international law. However, in 2018 the group declared its support for open, free and secure internet, thus promoting unfragmented global internet.

US as well as G7 and EU countries tend to view the internet as a free-flowing entity that is largely driven by market competition along with the support and regulation of the government and the participation of civil society [Basu A. et al., 2018]. However, we find historically that the narrative of *laissez-faire* has been used by the US and other capitalist countries to create new colonies based on consumption patterns. Today, data colonialism is being perpetuated under the aegis of the free market.

4. India's Emerging Role in Shaping Cyberspace Norms

India has historically played an active role in advocating the interests of the developing world at various venues such as the United Nations Convention on the Law of the Sea (UNCLOS) [Hiranandani G., 2000], the nuclear

non-proliferation regime [Kumar A., 2014], the international regime of the peaceful uses of outer space, and many more [Rao P., 2015]. Today, India has once again an excellent opportunity to play a central role in the debate about cyberspace as a key issue of national security. India must assume the leading role in this regulatory process, as many developing countries look towards it as a country without any bias towards either the US or the Sino-Russian cyber policy. As in the 2017 norm formulation process, the US and Russia proposed two resolutions that were passed by the UNGA First Committee on Disarmament and International Security at 73rd Session of the United Nations General Assembly, 2019). India voted for both of them, opening a new opportunity for proactively shaping norm formulation in keeping with the requirements and agendas of developing countries.

India's unbiased approach is deeply based on its constitutional values, in which individual rights are seen as a collective good. For example, when we talk about data protection, we refer not only to the protection of individuals' data but also to a system that would foster an environment for a free and fair digital economy. Unlike China, where the state sees itself above the individual, or US and European countries, where liberty is considered as freedom from state control and individuality is the focus of constitutional values, India sees the protection of personal data and the data economy as being complementary to each other, insofar as collective interest lies in individual interest. Therefore, India is fraying a way to protect individual rights while promoting the digital economy. As we saw, Free Basics sponsored by Facebook experienced a setback in India, checking the colonial approach of private US organizations.

Still, India should not further postpone its data regulatory framework. In a recent 2021 development, the mobile IP messaging application WhatsApp sought consent from users to share their data, including transaction data and location details, with Facebook, which means WhatsApp will share its users with Facebook, despite the latter being criticized for the Cambridge Analytica Scam. The Indian government sent 14 queries to WhatsApp and posted a note to protect Indian users from being exposed to greater security risks. Moreover, India banned 267 Chinese apps that have constantly mined Indian user data without proper consent and thus became a threat to national security as per reports received from the Indian Cyber Crime Coordination Center of the Ministry of Home Affairs. Thus, India has protected itself from data colonialism by private companies as well as vicious agendas hidden in state policies. India should not delay adopting a Personal Data Protection Act to protect its citizens from threats, as such companies thrive only in the context of lawlessness.

Cybersecurity and cyber laws are coupled to each other. To make a secure cyberspace, space laws and regulations should be framed in such a manner that any violator receives appropriate punishment. As cyberthreats are not exclusively internal but can come from any corner of the world, the IT Act of 2000 (amended in 2008) has largely become ineffective. The recent security breach at the Kundakulam Nuclear Power Plant has raised serious concerns, all the more so as it was not handled properly: the administration of the Nuclear Power Corporation of India Ltd. (NPCIL) initially denied the incident, and the North Korean hacker was not even traced [Madhavan N., 2019].

Most IT-related issues are covered by the Information Technology Act of 2008. However, despite its comprehensive nature, this act does not deal with all offenses or provide sufficient punishment for them. For example, section 66E of the act that concerns breaches of privacy stipulates only three years of punishment and a fine of two lakh rupees [Pathak U., 2017]. In addition, the act does not deal comprehensively with the ways of tackling international threats.

Hence, India should frame its cyber policies in a way that would allow it to trace and attribute cyberattacks. Many non-state actors such as tech companies and hackers are getting engaged in cyberspace architecture, and India must work to develop a cohesive approach to the regulation of cyberspace. As the Ministry of External Affairs (MEA) cannot deal with private organizations directly, India should push its private organizations to take part in the process.

Conclusion

The last national Cybersecurity Policy was adopted in 2013. It is high time to update it, as the world has greatly changed and is getting ready for a new digital revolution following the Covid-19 pandemic, with the cyberspace playing an increasing role in our daily life.

India should create a body with stakeholders from the Defense Ministry (DM) and the MEA, as both of these ministries have roles in cyber defense and cyber strategy. It should also involve security researchers and representatives of the private sector, civil society and the military to shape a better cyber strategy.

Just as regular military exercises take place with multiple countries, India should conduct cybersecurity exercises with different nations, especially developing countries when it could help in capacity building.

India's cybersecurity should become an essential part of its national security.

India should clearly define how international laws apply to cyberspace.

Though India already has a strong cybersecurity infrastructure, it should keep upgrading it as well as conducting hackathons to improve it.

India should promote the participation of the private sector in creating a safer cyberspace.

References

Appadurai A. (1991) Global ethnoscapes: Notes and queries for a transnational anthropology. In: R. Fox (ed.) Recapturing Anthropology. Santa Fe: School of American Research Press, pp.191–210.

Basu A., Hickok E., Rathi A., Trikanad S. (2018) Cyberspace and External Affairs: A Memorandum for India. Available at: https://cis-india.org/internet-governance/files/cyberspace-and-external-affairs (accessed: 14.02.2021)

Bhabha H. (1984) Of Mimicry and Man: The Ambivalence of Colonial Discourse. Available at: https://doi.org/10.2307/778467 (accessed: 04.06.2021)

Bhargava K. (2020) PM Modi's mantra for Atmanirbhar Bharat: Value-Addition to raw material, making finished goods. Available at: https://www.financialexpress.com/economy/pm-modis-mantra-for-atmanirbhar-bharat-value-addition-to-raw-material-making-finished-goods/2055739/ (accessed: 04.06.2021)

Brain J. (2021) The Cotton Industry. Historic UK. Available at: https://www.historic-uk.com/HistoryUK/HistoryofBritain/Cotton-Industry/ (accessed: 03.04.2021)

Brandom R. (2015) British "Karma Police" program carries out mass surveillance of the web. The Verge. Available at: https://www.theverge.com/2015/9/25/9397119/gchq-karma-police-web-surveillance (accessed: 07.02.2021)

Cheney-Lippold J. (2011) A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. Available at: https://doi.org/10.1177/0263276411424420 (accessed: 04.06.2021)

Cohen J. (2007) Cyberspace As/And Space. Available at: https://scholarship.law.georgetown.edu/facpub/807 (accessed: 04.06.2021)

Cyberspace as Global Commons: The Challenges. (2012) DATAQUEST., Available at: https://www.dqindia.com/cyberspace-global-commons-the-challenges-1/ (accessed: 04.03.2021)

Dijck J. van (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, no 2, pp. 197–208. Available at: https://doi.org/10.24908/ss.v12i2.4776 (accessed: 10.05.2021)

Dijck J. van, Poell T., Waal M. de (2018) The Platform Society. Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190889760.001.0001/oso-9780190889760 (accessed: 04.06.2021)

Ghosh S. & Kanter J. (2019) Google says data is more like sunlight than oil, just 1 day after being fined $57 million over its privacy and consent practices. Available at: https://www.businessinsider.in/google-says-data-is-more-like-sunlight-than-oil-just-1-day-after-being-fined-57-million-over-its-privacy-and-consent-practices/articleshow/67640224.cms (accessed: 4.06.2021)

Gitelman L. (2013) *"Raw data" is an oxymoron*. Cambridge: MIT Press, 192 p.

Haupt M. (2016) Data is the New Oil—A Ludicrous Proposition. Medium. Available at: https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294 (accessed: 26.02.2021)

Hauser-Schäublin K., Dickhardt M. (2003) Kulturelle Räume—Räumliche Kultur. Available at: https://www.lit-verlag.de/isbn/978-3-8258-6799-4 (accessed: 20.08.2020)

Hiranandani G. (2000) *Transition to Triumph: History of the Indian Navy, 1965–1975*. New Delhi: Spantech & Lancer. 415 p.

Ho W.-C. (2008).The Transcendence and Non-Discursivity of the Life world. *Springer Science + Business Media,* no 3, pp. 323–342.

Jasanoff S. (2004). Ordering knowledge, ordering society. In: States of Knowledge: The Co-production of Science and the Social Order. Available at: https://www.routledge.com/States-of-Knowledge-The-Co-production-of-Science-and-the-Social-Order/Jasanoff/p/book/9780415403290 (accessed: 04.06.2021)

Kokot W. (2007) Culture and Space — anthropological approaches. *Ethnoscripts* , no 9, pp. 10–23.

Kumar A. (2014) Norm Entrepreneur, Catalyst or Challenger? India in the Nuclear Non-proliferation Narrative. Available at: https://journals.sagepub.com/doi/abs/10.1177/0971523115592493 (accessed: 03.04.2021)

Latour B. (1987) Science in Action. Available at: https://www.hup.harvard.edu/catalog.php?isbn=9780674792913 (accessed: 04.06.2021)

Lindsay J. (2015) The Impact of China on Cybersecurity: Fiction and Friction. Available at: https://www.belfercenter.org/publication/impact-china-cybersecurity-fiction-and-friction (accessed: 04.06.2021)

Madhavan N. (2019) Is India cyber security ready? Available at: https://www.thehindubusinessline.com/opinion/columns/is-india-cyber-security-ready/article29911679.ece (accessed: 04.06.2021)

Mishra D., Chanchani M. (2020) Internet users in India: For the first time, India has more rural net users than urban. Available at: https://timesofindia.indiatimes.com/business/india-business/for-the-first-time-india-has-more-rural-net-users-than-urban/articleshow/75566025.cms (accessed: 04.06.2021)

Mozur P. (2015) New Rules in China Upset Western Tech Companies. Available at: https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html (accessed: 04.12.2021)

Roser M. (2018) The Internet's history has just begun. Available at: https://ourworldindata.org/internet (accessed: 4.06.2021)

Pathak U. (2017) Cyber security and cyber laws in India: focus areas and issue areas. Vol. 6, issue 1. DOI: 10.5958/2277-937X.2017.00008.9

Preeti (2016) Colonial codification of education in India until 1920. *Journal of Indian Education,* no 2, pp. 29–44.

Rao P. (2015) *From Fishing Hamlet to Red Planet: India's Space Journey.* Bengaluru: ISRO, 736 p.

Xi Jinping P.E. (2015) Remarks. Available at: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (accessed: 03.02.2021)

Said E. (2003) *Orientalism*. London: Penguin, pp. 1–28, 350–353.

Scholz L. (2018) Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies. Tennessee Law Review, vol. 85, p. 2020. DOI: 10.2139/ssrn.3252543

Segal A. (2016) China, Encryption Policy, and International Influence. Hoover Institution. Series Paper No. 1610. Available at: https://www.lawfareblog.com/china-encryption-policy-and-international-influence (accessed: 02.03.2021)

Segal A. (2020) China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *NBR Special Report,* no 87, pp. 85–100.

Sherman J. (2019) How Much Cyber Sovereignty is Too Much Cyber Sovereignty? Available at: https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty (accessed: 07.12.2021)

Singh S. (2013) Govt. Violates privacy safeguards to secretly monitor Internet traffic. Available at: https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece (accessed: 04.03.2021)

Thengadi D. (1998) *The third way*. Bengaluru: Sahitya Sindhu Prakashana, 283 p.

Venables A. (2019) Establishing Cyber Sovereignty — Russia Follows China's Example. Available at: https://icds.ee/en/establishing-cyber-sovereignty-russia-follows-chinas-example/ (accessed: 16.12.2020)

Young R. (1995) Foucault on Race and Colonialism, Available at: https://www.semanticscholar.org/paper/Foucault-on-Race-and-Colonialism-Young/b4677c88a97256945644050fb7b2a33b1700503a (accessed: 04.06.2021)

Problems of Typology of Armed Conflicts in Cyberspace

Sergei Garkusha-Bozhko

Legal Adviser, Saint Petersburg School of Higher Sportmanship in Water Sports. Address: 10/1 Grebnoy Channel Embankment, Saint Petersburg 197110, Russian Federation. E-mail: garkusha-bozhko.sergej@yandex.ru

Abstract

The development of information technologies in the modern world affects all spheres of human activity, including the sphere of military activities of states. The current level of development of military information technologies allows us to talk about a new fifth possible theatre of military operations, namely, cyberspace. The Tallinn Manual on International Law Applicable to Cyber Operations, developed in 2013 and updated in 2017 by experts from the NATO States, also confirms the likelihood of armed conflict in cyberspace. It is indisputable fact that cyber operations committed in the context of an armed conflict will be subject to the same rules of International Humanitarian Law that apply to such armed conflict. However, many cyber operations that can be classified as military operations may be committed in peacetime and are common cybercrimes. In such circumstances, it is imperative to distinguish between such cybercrimes and situations of armed conflict in cyberspace. Due to the fact, that there are only two types of armed conflict — international and non-international, this problem of differentiation raises the question of the typology of armed conflicts in relation to cyberspace. The main questions within the typology of cyber armed conflicts are: whether an international armed conflict can start solely as a result of a cyber-attack in the absence of the use of traditional armed force; and how to distinguish between ordinary criminal behaviour of individuals in cyberspace and non-international armed conflict in cyberspace? The purpose of this article is to provide answers to these urgent questions. The author analyses the following criteria that play a role in solving the above problems: criteria for assigning a cyber attack to a state and equating such a cyber-attack with an act of using armed force in a cyber armed conflict of an international character; and criteria for the organization of parties and the intensity of military actions in a non-international cyber armed conflict. Based on the results of this analysis, the author gives relevant suggestions for solving the above issues.

Keywords

cyberspace; Tallinn Manual; International Humanitarian Law; armed conflict; cyber-operation; cyber-attack.

For citation: Garkusha-Bozhko S. Yu. (2021) Problems of Typology of Armed Conflicts in Cyberspace. *Legal Issues in the Digital Era*, no 2, pp. 82–103.

DOI: 10.17323/2713-2749.2021.2.82.103

Introduction

The development of information technologies affects all spheres of human activity and the military activity of states is not an exception. The current level of development of military technologies allows us to speak about possible spread of military operations to cyberspace. In other words, in the modern world, an armed conflict in cyberspace is no more an invention of science fiction writers and screenwriters of fantastic entertainment films — now it is a potential conflict that can begin due to the collision of interests of two or more states in the cybersphere. The likelihood of such a conflict is also recognized in the statement of Russian President Vladimir Putin, who noted that "one of the main strategic challenges of our time is the risk of a large-scale confrontation in the digital sphere."[1]

As noted in the doctrine [Melzer N., 2017: 51], cyberspace is now "the fifth domain of warfare" after land, sea, air and outer space. This statement cannot be challenged for the reason that, due to the level of development of modern technologies, cyberspace is, in fact, a potential theater of military operations. The high likelihood of such armed conflicts forced states to think about the legal regulation of such conflicts, and in 2013, thanks to the efforts of lawyers and military specialists from NATO countries, with the participation of specialists from the International Committee of the Red Cross (ICRC), the Tallinn Manual on the International Law Applicable to Cyber Warfare was adopted.

This Manual is an attempt to develop norms of international law applicable not only to this type of armed conflict, but also to cyberspace in general, both in wartime and in peacetime. The need for this kind of international law is very high, which led to the adoption of a new expanded version of this manual in 2017 (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations).

The key point in the application of international humanitarian law to cyberspace is the fact that cyber operations are carried out in the context of an armed conflict or in connection with it. This conclusion is not contested in

[1] Vladimir Putin on the complex set of measures to restore Russian-American cooperation in the field of international information security. Available at: URL: http://kremlin.ru/events/president/news/64086 (accessed: 01.04.2021)

the doctrine [Droege C., 2014: 12]; [Streltsov A.A., 2014: 84]; [Schmitt M., 2002: 133]; [Schmitt M., 2019: 334]; [Schmitt M.. 2014: 191]; [Döge J., 2010: 491]. In other words, cyber operations carried out in the context of an armed conflict would be governed by the same rules of IHL as this conflict.

However, despite the obviousness of the above conclusion, many cyber operations that can be qualified as military operations in cyberspace can be carried out in the absence of any armed conflict. For example, we often see media reports of cyber attacks or acts of cyber terrorism that take place in times of peace[2]. In addition, various cyber operations can be trivial cyber crimes. As we know, there is already an international treaty addressing the cybercrime — the Convention on Cybercrime (Budapest, 2001).[3]

The above examples of hostile cyber operations emphasize the problem of their delimitation from armed conflicts in cyberspace. This problem can also be illustrated by an example where cyber operations are the only hostile actions carried out against a particular state.

We are talking here about such an example as the Stuxnet virus, which was aimed at disrupting the normal operation of a uranium enrichment plant in the Islamic Republic of Iran, the city of Netense. This case is one of the clearest examples of long-term hostile impact on state information systems. As it was later established, this virus was developed with the participation of experts from the security services of the United States and Israel, and its goal was the Iranian nuclear program.[4]

States, in particular Iran, did not qualify this situation related to the Stuxnet virus as an armed attack. However, the legal doctrine suggested that if a certain state was behind this virus, this situation can be qualified as an international armed conflict in cyberspace [Schmitt M., 2012: 252]. Thus, G. Brown explicitly states that the Stuxnet virus is a cyber attack, since it represents violation of the fundamental international legal principle of the non-use and threat of force, as well as in violation of *jus in bello* [Brown G., 2011: 71]. Based on such statements in the doctrine, the

[2] See, e.g. DDoS-attacks on the web-sites of the Ministry of Internal and KGB of the Republic of Belarus. Available at: https://iz.ru/1045947/2020-08-09/v-belorussii-soobshchili-o-ddos-atakakh-na-saity-kgb-i-mvd (accessed: 01.04.2021). Cyber-terrorists attacked the computers of Rosneft Oil Company. Available at: https://tvzvezda.ru/news/vstrane_i_mire/content/201706271530-owel.htm (accessed: 01.04.2021)

[3] Budapest Convention on Cybercrime, 2001. European Treaty Series. No. 185.

[4] Stuxnet was work of U.S. and Israeli experts, officials say. Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (accessed: 01.04.2021)

thought may well arise about possible cyber attacks carried out by a non-governmental group against the government of a particular state, which will entail the question of the possible qualification of such a situation as a non-international armed conflict in cyberspace.

In such conditions, in order to solve this problem of delimiting situations of ordinary criminal cyber operations from situations of cyber armed conflicts, it is necessary to analyze the typology of such armed conflicts. As it is well known, there are only two types of armed conflict: international and non-international one. Their criteria are well enough studied and described in the doctrine, so we will not delve into the general typology of armed conflicts, but will limit ourselves to examining those aspects that poses problems to qualifying cyber operations in the context of armed conflicts. Let's start with an international cyber armed conflict.

1. International cyber armed conflict

Let's recall that, according to the Article 2 that is common for three Geneva Conventions of 1949, an international armed conflict means any case of "declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. "[5] This provision is the only treaty definition of an international armed conflict. Paragraph 4 of Article 1 of Additional Protocol I supplemented this definition, referring to this type of armed conflict also situations of armed conflict "in which peoples are fighting against colonial domination and alien occupation and against racist régimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations".[6]

However, one must assume that the struggle against colonialism is already a thing of the past, and the exercise of the right to self-determination by peoples is unlikely to take place in cyberspace. Therefore, we will not take this addition into account and will consider an international armed conflict solely as a situation where armed forces are used between sovereign states, as clearly indicated by the International Tribunal for the former

[5] Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field. 1949. UNTS 970.

[6] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I). 1977. UNTS 17512.

Yugoslavia[7]. The authors of the Tallinn Manual proceeded from the same message, stating in Rule 82 that "[cyber] international armed conflict occurs whenever military action occurs between two or more states, which may include or be limited to cyber operations" [Tallinn Manual 2.0, 2017: 379]. As can be seen from the above, the issue of qualifying an armed conflict, including a cyber conflict, as an international one depends on the very fact of such a conflict, and not on the fact that the parties recognize the state of an armed conflict.

The key problem of the legal qualification of an international armed conflict in cyberspace is the question of whether such an armed conflict can start solely as a result of a cyber attack in the absence of the use of traditional armed force? The solution to this issue is influenced by two main criteria: 1) attribution of a cyber attack to the state and 2) equating such a cyber attack with the use of traditional armed force. In other words, these criteria require an answer to questions about whether such a cyber attack is attributed to a particular state; and whether it leads to the same consequences as the traditional use of military force.

1.1. Attribution of a cyber attack

Let's start with the first criterion. On the one hand, the attribution of a particular cyber attack or cyber operation to a particular state is an intractable problem due to the anonymity of users in cyberspace. But, on the other hand, until it is established that states are both the perpetrators of this cyber attack and the victims of it, there can be no question of qualifying the situation as an international armed conflict.

Of course, it should be kept in mind that this problem is more factual than legal in its nature, and it is indicated in the legal doctrine [Droege C., 2014: 14]; [Zhang L., 2012: 804]; [Tsagourias N., 2012: 233]; [Döge J., 2010: 500–501]; [Hathaway O., Crootof R. et al., 2012: 856]. One of the proposed ways to solve this problem is to use legal assumptions [Lin H., 2012: 521]. For example, it must be assumed that a cyber attack is attributed to a state if it originated from IT infrastructure owned by the government of that state.

However, such an approach based on legal assumptions is not consistent with the norms of international law for the following reasons. First, the Articles on Responsibility of States for Internationally Wrongful Acts

[7] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-T. ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Para. 70.

(hereinafter — Articles on Responsibility of States) do not provide for the use of such assumptions for attribution of wrongful acts to a State[8]. In this regard, it is necessary to recall the decision of the International Court of Justice (ICJ) in the case «On oil platforms (Islamic Republic of Iran v. United States of America)», in which the Court established a sufficiently high threshold for attributing behavior to a state in the context of the right to self-defense. Specifically, the UN ICJ noted: «… the court must simply determine whether the United States has demonstrated that it was the victim of an" armed attack " by Iran in order to justify its use of armed force in self-defense; and the burden of proof of the existence of such an attack rests with the United States»[9].

Of course, this decision of the ICJ was made on the issue of the state's right to self-defense, i.e. in the context of *jus ad bellum*. However, we believe that this rule, derived by the International Court of Justice, is applicable to all questions of fact when attributing behaviour to a state, since attribution should be based on facts and not on assumptions. In addition, the attribution of a cyber attack to a state also raises questions, including in the context of the jus ad bellum, which once again proves the applicability of this ICS decision to cyberspace.

Second, the use of legal assumptions in relation to the attribution of cyber operations to a particular state is not possible due to the risks that exist in cyberspace. In particular, due to the risks of manipulation, the use of VPN technology and the possibility of remote control over the information system under a false name.

Of course, there is a point of view in the doctrine that the attribution of a cyber operation to a specific state is possible through the use of various intelligence data [Lin H., 2012: 522], however, it must be assumed that due to these risks, one cannot be completely sure of the reliability of such data.

Based on this, it is obvious that the burden of responsibility imposed on the state for all cyber operations carried out using the information infrastructure of such a state, in the absence of other evidence, would be excessive. This conclusion is also supported by the developers of the Tallinn Manual: in paragraph 13 of the commentary to Rule 15, which enshrined the regulation on the appropriation of cyber operations carried out by state

[8] Draft articles on. Responsibility of States for Internationally Wrongful Acts. Adopted by General Assembly Resolution No. 56/83 on 12.12.2001. Available at: https://undocs.org/pdf?symbol=ru/A/RES/56/83 (accessed: 01.04.2021)

[9] Oil Platforms (Islamic Republic of Iran v. United States of America). ICJ Judgment. 6 November 2003 // I. C. J. Reports. 2003. P. 161. Para 57.

bodies, the developers noted that «The mere fact that operations in cyberspace were launched or otherwise emanated from government infrastructure, or that malware used against a compromised information infrastructure is designed to "report" to another country's government infrastructure, is usually not sufficient evidence that that the operation should be assigned to the state. However, such use may serve as an indication that the State in question may be associated with the operation.» [Tallinn Manual 2.0, 2017: 91].

Another problem discussed in the doctrine [Droege C., 2014: 15]; [Backstrom A., Henderson I., 2012: 503, 505], arising in the framework of attribution of a cyber attack to the state, is the problem of appropriation of cyber attacks by the state, committed by private individuals, or as they are also called in the media — hackers or hacker groups. This problem is of particular importance in cyberspace due to the prevalence of user anonymity in it. Let us turn to the Articles on State Responsibility, Article 8 of which stipulates the following: «The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct».[10]

When analyzing this rule of the Articles on State Responsibility, the question arises: what does the wording «under instructions or under the direction or control» mean? In this regard, the International Court of Justice noted that in order for the conduct of an individual or an organized group to be attributed to the state, the state must exercise effective control over the operation during which the alleged offenses were committed, which must be demonstrated in relation to all unlawful acts committed by such individuals.[11] If such effective control is not exercised by the state over a specific operation, then such an operation cannot be attributed to such a state, even if this operation was carried out by a person (group of persons) whose degree of dependence on the authorities of such a state was very high.[12]

[10] *Draft articles* on. *Responsibility* of *States* for Internationally Wrongful Acts. Adopted by General Assembly Resolution No. 56/83 on 12.12.2001. Available at: https://undocs.org/pdf?symbol=ru/A/RES/56/83 (accessed: 01.04.2021)

[11] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits. ICJ Judgment of 27 June 1986 // I.C.J. Reports 1986. P. 14. Para 115–116; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). ICJ Judgment of 26 Feb. 2007 // I.C.J. Reports. 2007. P. 43. Para 400 — 406.

[12] Military and Paramilitary Activities in and against Nicaragua… Para. 115

The United Nations International Law Commission (UN ILC), in para 3 of its commentary on Article 8 of the Articles on State Responsibility, spoke in the same vein: the UN ILC points out that attributing conduct to a state in accordance with Article 8 requires that the state be in control of a particular operation and that the conduct in question must be an integral part of that operation.[13]

The International Criminal Tribunal for the former Yugoslavia has taken a completely different view on this issue. In particular, in the decision of his Appeals Chamber in the well-known Tadić case, he stated that if a group, such as a rebel armed group, has a degree of organization sufficient for a certain state to exercise so-called «general control» over such an organization with the necessary level of organization and hierarchical structure, then it is not necessary to establish the fact of effective control over specific operations — to attribute the behaviour of such a group to the state, general control is sufficient.[14] However, the ICTY also added to the above statement that if the state exercising control is not a territorial state, then more extensive and conclusive evidence is needed that the state does exercise control over individuals and groups, and this means that the participation of such a state in the leadership the operations of such individuals and groups will be difficult to demonstrate.[15]

In response to this statement by the ICTY, the International Law Commission, in para 5 of the commentary to Article 8 of the Articles on State Responsibility, noted that the question of the degree of control on the part of a particular state over certain behaviour, which is necessary for attributing such behaviour to a state, should be decided on the basis of actual circumstances of each individual case.[16]

Of course, the above discussion is not directly related to cyberspace. However, it must be assumed that this discussion sets out the basic principles that should be followed when deciding the question of attributing the behaviour of individuals to the state. In our opinion, there is no reason to deny their applicability to cyberspace, in particular, to the issue of

[13] ILC Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Adopted in 2001 // Yearbook of the International Law Commission. 2001. Vol. II. Part Two. P. 47.

[14] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-A. ICTY Appeals Chamber Judgement of 15 July 1999. Para 120.

[15] Ibid. Para 138–140.

[16] ILC Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Adopted in 2001 // Yearbook of the International Law Commission. 2001. Vol. II. Part Two. P. 48.

appropriation of cyber operations. The problem here lies elsewhere — in the issue of identifying such individuals — due to the already mentioned problem of anonymity, it will be quite difficult to establish them for sure, and this difficulty, most likely, will lie in assessing the actual circumstances of the cyber operation.

Obviously, one of the solutions that can be proposed here is to involve technical specialists to solve the problem of anonymity. However, in our opinion, this will not be enough for the reason that there is still little interstate practice in this field, from which it would be possible to derive specific criteria for attribution of behavior in cyberspace. Therefore, in such a situation, states need to develop appropriate practice on this issue.

1.2. The use of armed force

Let's move on to the second criterion, which must be satisfied in order to establish the fact of the existence of an international armed conflict in cyberspace — to the criterion of the use of armed force between two or more states.

Before starting the study of this criterion, it is necessary to make the following remark. It is important to note that the classification of a conflict as an international armed conflict in accordance with *jus in bello* (international humanitarian law) must be separated from issues governed by *jus ad bellum*. Let us explain why it is important to make such a distinction.

It should be borne in mind that within in terms of application of *jus ad bellum* to cyberspace, the key issue is whether a cyber attack is an act of use of force in accordance with para 4 of Article 2 of the UN Charter, and if so, under what circumstances; and is it an act of armed attack (an act of aggression) in accordance with Article 51 of the UN Charter, and under what circumstances does it legitimize the right of the victim state to self-defense? These are the main problems discussed in the doctrine in relation to the application of jus ad bellum to cyberspace [Roscini M., 2010: 85–130]; [Schmitt M., 1998-1999: 885-937]; [Lin H., 2010: 63–86].

The developers of the Tallinn Manual proceeded from the same logic of differentiation between *jus ad bellum* and *jus in bello* — they dedicated a separate chapter to jus ad bellum: norms 68 to 75 [Tallinn Manual 2.0, 2017: 328–356]. In turn, we recall *that jus ad bellum* and *jus in bello* have different subjects of regulation: the subject of *jus ad bellum* is interstate relations with respect to the lawful use of force in relations between states; and the subject of *jus in bello* is interstate relations with respect to the conduct of

parties to an armed conflict and to the protection of victims of armed conflicts. Therefore, when qualifying an international armed conflict, an action is considered as an act of the use of armed force without prejudice to the question of whether such an action is an act of use of force in accordance with para 4 of Article 2 of the UN Charter (most often such acts are the use of force in accordance with this rule) or an act of aggression in accordance with Article 51 of the UN Charter. This distinction between *jus ad bellum* and *jus in bello* also applies to cyberspace.

Returning to international humanitarian law, we have to note that international treaties in this field do not enshrine the concept of "an act of the use of armed force". This issue, in fact, is attributed to the sphere of judicial practice — usually various international and national courts decide this issue. Let us try to deduce the doctrinal concept of the use of armed force in IHL.

The ancient Chinese philosopher Sun Tzu in his famous treatise «The Art of War» very accurately described the goal of military operations — «to defeat the enemy and increase strength» [Sun Tzu, 2016: 59]. Indeed, the goal of any armed conflict is victory over the enemy side, and to achieve this goal, the parties use weapons or means of military action, as it is called in international humanitarian law. In a classic armed conflict, the use of various traditional means and methods of military operations, in fact, is the use of armed force. However, as we know, cyber attacks are in no way connected with the use of such means and methods. Therefore, the question arises: what is considered to be the use of force in cyberspace in the context of an international armed conflict?

When thinking about this question, one of the first thoughts that arise is to compare the consequences of a cyber attack with the consequences of using «traditional» means of warfare. There is a unanimous opinion in the doctrine that if a cyber attack is assigned to a certain state and leads to the same consequences as the «classical» use of armed force, then such a situation must be qualified as an international armed conflict [Droge K., 2014: 18]; [Schmitt M., 2012: 251]; [Dinniss H., 2012: 131]; [Melzer N. 2011: 24]; [Backstrom A., Henderson I., 2012: 504]; [Hathaway O., Crootof R. et al., 2012: 848]. Niels Melzer also points out that "cyber operations sponsored by a state will lead to the outbreak of an international armed conflict if they are aimed at causing harm to another state, not only by directly causing death, injury or destruction, but also by a direct negative impact on its military operations or military potential "[Melzer N., 2011: 24].

In turn, let us express our agreement with this point of view, since it is quite logical to classify a situation as an international armed conflict when

a cyber attack leads to the infliction of death or injury to people, or to the infliction of harm or destruction of various physical objects. We also agree with the expanded point of view of N. Melzer, since based on the general goal of any armed conflict — to weaken and defeat the enemy, the impact on his military potential, including through cyber attacks, similarly plays an important role in the qualification of the situation, as an international armed conflict.

However, with all the effectiveness of this «consequences approach», it seems insufficient in terms of fixing the entire range of possible consequences of cyber operations and the harm they can cause. The point is that not all the consequences of cyber operations in the physical world will be similar to the consequences of the use of traditional weapons. It should be borne in mind here that sometimes cyber operations, including cyber attacks, are not aimed at physically destroying or damaging civilian or military infrastructure, but most often are aimed at disrupting its functioning. For example, cyber operations can be carried out with the aim of manipulating certain infrastructure. Moreover, a hacker carrying out such a cyber operation will try to do everything to ensure that this cyber operation goes unnoticed.

Examples of such cyber operations include cyber attacks aimed at manipulating the information systems of large banks in order to harm the financial system of a state or aimed at manipulating the energy sector in order to harm the energy system of such a state.[17]

At first glance, cyber attacks, even in the absence of the use of traditional weapons, inflict damage on the population of such a state comparable to the consequences of the use of armed force. However, in such situations, victim states often do not qualify such cyber operations as military aggression in order to avoid confrontation in the international arena (as well as, possibly, for other reasons). In fact, in cases of cyber attacks against them, states remain silent, and thus, do not form any practice. Based on this, the formulation of any legal position on this issue seems to be rather complicated. However, in the absence of state practice, the following options for possible solutions to this problem can be proposed.

The first option suggests considering any hostile cyber operation that negatively affects any infrastructure as an act of using military force. Such

[17] See e.g.: FSB reported cyber-attacks on Russian banks. Available at: URL: https://www.bfm.ru/news/340401 (accessed: 10.04.2021); Hackers attack Russian banks Available at: URL: https://www.gazeta.ru/tech/2020/02/18/12965743/bank_energy.shtml (accessed: 10.04.2021)

an approach will not contradict the norms of international humanitarian law due to the absence of a threshold of violence at which an international armed conflict takes place. Moreover, the well-founded desire to close the legal gap in the protection of the civilian population in the first place is also an argument in favour of this approach. In addition, based on the cyber security strategies of various countries, it can be concluded that states attach great importance to the protection of their main strategic infrastructures in cyberspace.[18] Therefore, it is entirely possible to assume that states could qualify a cyber attack aimed at disrupting the functioning of their strategic infrastructures as an armed attack. In this regard, N. Melzer proposes the concept of critical infrastructure in order to determine the "scale and impact" of a cyber attack on an information network, which will help in establishing the fact of an act of aggression in accordance with Article 51 of the UN Charter [Melzer N., 2011: 14].

The second option proposes not to focus solely on the consequences of a cyber operation, but to take into account a number of factors that determine whether it was an act of the use of armed force. These factors, in addition to the consequences of a cyber operation, must also include the technical means for the implementation of this cyber operation; the fact of participation in the implementation of this operation by a military department (in particular, cyber troops) or another body of the state; the duration of such an operation; and the nature of the target — whether it was a military or civilian target.

The above factors are not invented by chance — they also play a role in determining the fact of the use of armed force in its traditional sense. As

[18] See: Information Security Doctrine of Russian Federation. Adopted 5.12.2016. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed: 05.04.2021); Conception of Cybersecurity of Belarus. Adopted 18.03.2019. Available at: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (accessed: 5.04.2021); Défense et sécurité des systèmes d'information. Stratégie de la France. Available at: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (accessed: 11.04.2021); GSchutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7 (accessed: 10.05.2021); Canada: Stratégie nationale sur les infrastructures essentielles. Available at: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx (accessed: 12.01.2021); The UK Cyber Security Strategy. Published on 25 November 2011. Available at: https://www.gov.uk/government/publications/cyber-security-strategy; National Cyber Strategy of the United States of America. Adopted in September 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. (accessed: 12.01.2021)

an example, let us give the following situation: if, suppose, the commander-in-chief of a state was killed as a result of an aerial bombardment by the air forces of another state, then this, of course, would be the use of armed force, and we can talk about the existence of an international armed conflict. But in the case of killing such a person by infecting him, for example, with anthrax, the spores of which were sent to him by a letter from another state, it is difficult to ascertain the existence of an armed conflict. Pointing out this most important factor of the difference between hostile acts committed by the armed forces, on the one hand, and hostile acts committed by other bodies of the state, on the other hand, it should be noted that in this regard M. Sassoli and A. Bouvier noted: "When the armed forces of two states are involved, one shot or one captured (according to government instructions) is enough for IHL to be applied, although in other cases (for example, an execution carried out by a secret agent sent by his government abroad), a higher threshold of violence is required "[Sassoli M., Bouvier A., 2008: 117].

Returning to cyberspace, it should be assumed that states will be more "sensitive" to cyber attacks directed against the information networks of their military and other state infrastructures than to cyber attacks against civilian networks. This conclusion finds its support in the doctrine [Droege C., 2014: 20]. Of course, this approach seems strange, but let's agree with it, because Governments will naturally focus primarily on the cybersecurity of their military and other public infrastructures. However, let us add to this conclusion: if a cyber attack directed against a civilian object results in civilian casualties or injury to civilians, states are likely to recognize the cyber attack as an act of military force as well. Therefore, this conclusion about the "sensitivity" of various information infrastructures for states should be taken conditionally.

Particular attention in the context of the use of force also needs to be paid to the nature and duration of a hostile cyber operation. Let's note that if a cyber attack is of a targeted nature and is not long-lasting, it will be possible to recognize it as an act of using armed force only if it has led to particularly destructive consequences. Returning in this regard, for example, to the Stuxnet virus, we have to note that it indicates that cyber attacks, sometimes, for a long time, are the only hostile actions against another state without the use of other traditional acts of the use of armed force, especially in situations of anonymous cyber attacks. Based on a comparison of the consequences, we can conclude that in the situation the Stuxnet virus was the use of armed force, because, as it was established, this virus led to the destruction of about a thousand IR-1 centrifuges at the uranium

enrichment plant in Netenze, Iran.[19] Based on this fact, many researchers came to the conclusion that this cyber attack can be considered an act of using armed force [Schmitt M., 2012: 252]; [Brown G., 2011: 71]. However, as you know, the Islamic Republic of Iran did not qualify these hostile acts in cyberspace as an act of using armed force. This position of Iran is quite understandable. It is one thing when a given plant could be destroyed as a result of an aerial bombardment by the air forces of another state, and this, unambiguously, would be the beginning of an international armed conflict; and it is quite another matter when the attack was cybernetic, there was no information about other cyber attacks, and the damage was limited only to the destruction of these centrifuges at nuclear installations — such a situation hardly meets the criterion of using armed force to reach the level of an international armed conflict. Therefore, Iran did not consider this situation as the use of armed force.

Of course, all of the above approaches are purely theoretical, and due to the lack of relevant state practice, it remains to be seen under what conditions states will qualify a cyber attack directed against them as an act of using armed force. It is clear that, for example, in the case of a cyber attack against the banking system of a state, even in a situation where such a cyber operation led to serious economic losses, such a cyber attack is outside the object and purpose of the use of armed force. But in the case of a cyber attack against electricity and water supply systems of the population and other vital infrastructures, which led to long-term hardships of the civilian population, it is quite possible to consider it as the use of armed force. Of course, in such a case, the impact of a cyber attack does not equate to the consequences of the traditional use of force, however, such a cyber attack leads to consequences from which the civilian population is guaranteed the protection afforded by the rules of international humanitarian law.

However, for all the importance of the position of states on the qualification of cyber attacks, it should be recalled that the rules of IHL apply regardless of whether states qualify a situation as an armed conflict or not — international humanitarian law applies in all cases of the actual existence of an armed conflict.

---

[19] Stuxnet was work of U.S. and Israeli experts..; Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? ISIS Report. 22 December 2010. Available at: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed: 20.04.2021); Obama Order Sped Up Wave of Cyberattacks Against Iran. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (accessed: 30.12.2020)

States simply cannot avoid applying such rules by declaring that there is no international armed conflict. Such "tricks" on the part of states, as you know, were suppressed even during the development of the Geneva Conventions of 1949, which was expressed in the content of common article 2: "... this Convention will apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, *even if the state of war is not recognized by one of them*"[20] (emphasis is mine. — S. G.-B.).

Let us also remind that in a commentary to this rule, ICRC lawyers noted the following: "... A state, committing a hostile act towards another state, can always pretend that it is not waging a war, but only carries out a police action or acts in the framework of lawful self-defense. The expression "armed conflict" complicates such disputes. Any disagreement arising between states and leading to the intervention of the armed forces is an armed conflict [...], even if one of the parties denies the existence of a state of war" [Pictet J., 1952: 32]. For all the importance of this comment, it is also important to take into account the presence of the *animus belligerendi*: some situations will not be considered an international armed conflict due to the fact that the necessary level of tension has not been reached in them, in particular, due to the absence of the *animus belligerendi*. This is noted in various national guidelines on the application of IHL. Therefore, random border clashes between the armed forces of different states will not be considered an international armed conflict.[21]

Obviously, in international humanitarian law, the existence of an international armed conflict does not depend on the qualifications of such situations by the parties to such a conflict. However, it must be assumed that in the case of international armed conflicts in cyberspace, due to the fact that cyberspace is a new theater of operations, many issues of qualifying such an armed conflict, in particular, issues of attribution of hostile behavior in cyberspace to a state and issues of the use of force, will depend on from the practice of states, which, unfortunately, has not yet been formed.

Let us now turn to consideration of the problematic of cyber non-international armed conflicts.

---

[20] Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field...

[21] See, e.g.: The UK Joint Service Manual of the Law of Armed Conflict. Joint Service Publication 383, 2004. Promulgated as directed by the Chiefs of Staff. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf. Para. 3.3.1 (accessed: 05.04.2021)

2. Cyber non-international armed conflict

The key rule for non-international cyber armed conflicts is rule 83 of the Tallinn Manual: "A non-international [cyber] armed conflict occurs whenever there is prolonged armed violence, which may include or be limited to cyber operations between government armed forces and organized armed groups or between such groups. The confrontation must reach a minimum level of intensity, and the parties involved in the conflict must have a minimum degree of organization" [Tallinn Manual 2.0, 2017: 385].

A key question in relation to this rule is how to distinguish between ordinary criminal conduct of individuals in cyberspace and non-international armed conflict in cyberspace? There are frequent reports in the media in which the actions of hackers and hacker groups, in particular such well-known ones as Wikileaks and Anonymous, are characterized as "cyber war".[22] Of course, such journalistic publications do not mean an armed conflict of a non-international character in the legal sense of the word. However, it is necessary to establish criteria for qualifying the situation as a non-international cyber armed conflict.

As is known, there is no definition of a non-international armed conflict in international treaty law. Therefore, this issue remained in the sphere of the doctrine and practice of states, on the basis of which the ICTY gave the following definition of an armed conflict of a non-international character: "An armed conflict [of a non-international character] occurs whenever ... there is a prolonged armed conflict between government forces and organized armed groups or between such groups within one state".[23]

The above norm of the Tallinn Guidelines is based on this definition proposed by the ICTY. Based on this, there are two criteria necessary to qualify a situation as a non-international armed conflict: the criterion for the intensity of violence and the criterion for the minimum level of organization of the parties. Let's start with the last criterion.

---

[22] WikiLeaks: Threat of cyberwar. Available at: http://rapsinews.ru/international_publication/20101130/251133841.html (accessed: 15.04.2021); Anonymous declared cyberwar to the Islamic State Available at: https://www.vesti.ru/hitech/article/625187 (accessed: 15.04.2021); WikiLeaks backlash: The first global cyber war has begun, claim hackers. 2010. December 11. Available at: https://www.theguardian.com/media/2010/dec/11/wikileaks-backlash-cyber-war (accessed: 15.04.2021); Anonymous: Protesters or Terrorists? Fog of cyberwar obscures truth. 2012. February 21. Availavle at: https://www.rt.com/usa/anonymous-freedom-cyber-wall-875/ (accessed: 15.04.2015)

[23] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-T. ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Para 70.

2.1. Organization of the parties

For an armed group to be considered organized and to be qualified as a party to a non-international armed conflict, it is required that it has a level of organization that will enable it to engage in continuous hostilities and comply with international humanitarian law. The hallmarks of such a necessary organization are the existence of an organizational chart that defines the command structure and authority over the military operations in which the group participates; the ability to recruit and train new members; and the existence of internal discipline rules. These signs are confirmed by judicial practice.[24] It is important to note that such an armed group is not required to have the same level of organization as the government's armed forces. However, such a group must have a certain hierarchy, level of discipline and the ability to comply with IHL norms. This is also confirmed by the practice of the ICTY.[25]

When these criteria of organization are analyzed for their applicability to hacker groups, the question arises as to whether such groups, organized exclusively in cyberspace, can be organized armed groups in accordance with international humanitarian law? In connection with this issue, M. Schmitt pointed out that "members of virtual groups may have never met and do not even know each other's real names. However, such groups can act in a coordinated manner against the government (or an organized armed group), receive orders from the virtual leadership, and be highly organized. For example, one [member] of the group may be tasked with identifying the vulnerabilities of the target [information] system, the second may develop malicious software to target these vulnerabilities, the third may carry out [cyber] operations, and the fourth may provide cyber defense against oncoming [cyber -] attacks" [Schmitt M., 2012: 256].

However, M. Schmitt also adds to this passage that the requirement for an organized armed group to have some form of responsible command and the requirement for its ability to comply with international humanitarian law are likely to be an obstacle to qualifying hacker groups as organized armed groups in terms of IHL. In addition, M. Schmitt adds that

[24] Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para. 199–203; Prosecutor v. Fatmir Limaj et al. Case № IT-03-66-T. ICTY Trial Chamber Judgement of 30 November 2005. Para 94–134; Prosecutor v. Ramush Haradinaj et al. Case № IT-04-84-T. ICTY Trial Chamber Judgement of 3 April 2008. Para 60.

[25] Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para 202.

it is difficult to imagine a situation where an effective system of discipline will be created within a hacker group, including in order to ensure that such a group complies with the norms of international humanitarian law [Schmitt M., 2012: 257].

A similar point of view is supported by the head of the ICRC Legal Department, Cordula Droege [Droege C., 2014: 24]. A similar opinion is expressed by most of the developers of the Tallinn Manual. In particular, para 13–15 of the Commentary to Rule 83 indicate that it is unlikely that hacker groups and groups associated exclusively with virtual messages will have an appropriate degree of organization, a responsible command, an appropriate hierarchy and an effective discipline system in order to could be considered as a party to an non-international armed conflict [Tallinn Manual 2.0, 2017: 390–391].

Of course, the above point of view is quite reasonable, but let's not rush to agree with it. In our opinion, the rapid development of information technology makes it possible for hacker groups to meet the criterion of organization: it cannot be ruled out that a highly organized hacker group could be created with responsible command and an appropriate degree of hierarchy, as well as a clear disciplinary system. The problem lies not in this possibility, but in the fact that at the moment there have been no examples of such highly organized hacker groups, or rather, states have not yet encountered such hacker groups in practice.

Of course, one can speculate that well-known hacker groups such as Anonymous can satisfy the criterion of being organized. However, due to the lack of detailed information about the structure of such a group, which, in turn, is due to the anonymity that rules in cyberspace, such hasty conclusions cannot be drawn.

Summing up the reflections on the compliance of hacker groups with the criterion of organization, it can be noted that the key problem here is not the potential possibility or impossibility of such compliance, but in the very absence of relevant state practice. Let us now turn to the next criterion — the intensity of hostilities.

2.2. Intensity of hostilities

The key question in relation to the intensity criterion is whether the use of cyber-only means can achieve the level of intensity required to qualify such a situation as a non-international armed conflict?

When characterizing the criterion of intensity in relation to classical non-international armed conflicts, it should be noted that the ICTY point-

ed out a number of factors that must be taken into account when assessing a specific situation in terms of intensity.

In particular, this is the use of the armed forces, rather than the police and other law enforcement agencies; the collective nature of hostilities; the severity of the attacks; an increase in the number of armed clashes, their territorial coverage and duration; the number of civilians forced to leave the conflict zones; distribution of weapons between the parties to the conflict; the types of weapons used, in particular, the fact of the use of heavy weapons is important; and the degree of destruction and the number of casualties caused by such armed clashes.[26] The question arises about the applicability of these factors to cyber attacks.

Probably, the consequences approach should be applied in a similar way. At first glance, there is no reason to assert that cyber operations cannot lead to such consequences that would make it possible to speak of the necessary level of intensity to qualify the situation as a non-international cyber armed conflict.

However, as C. Droege notes, cyber operations by themselves do not lead to many of the consequences-indicators of the intensity of violence. In her opinion, cyber operations will most likely lead to consequences that are serious enough to reach the required level of intensity, such as large-scale destruction or catastrophic consequences for a large part of the population due to repeated attacks [Droge C., 2014: 25].

In turn, we note that it can be argued that in order to achieve the required level of intensity, it is necessary that the consequences of cyber operations be comparable to the consequences of classical military actions, but at the same time it is necessary to take into account the fact that a cyber attack still will not lead to the same consequences as the traditional use of armed force. It should also be borne in mind that this conclusion is again purely theoretical — due to the lack of relevant practice of states, we have yet to see exactly what circumstances will satisfy the required level of intensity to qualify the situation as a non-international cyber armed conflict.

Conclusion

Summing up, the following can be noted with regard to the problem of the typology of armed conflicts in cyberspace. Of course, in a situation

[26] Prosecutor v. Fatmir Limaj et al. Case № IT-03-66-T. ICTY Trial Chamber Judgement of 30 November 2005. Para 135–170; Prosecutor v. Ramush Haradinaj et al. Case № IT-04-84-T. ICTY Trial Chamber Judgement of 3 April 2008. Para. 49; Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para 177–178.

where cyber operations are carried out in the context of an armed conflict (international and non-international), the same rules of international humanitarian law will apply to them as to the desired armed conflict.

As for a purely cyber armed conflict, both international and non-international, without the use of any traditional armed forces, such a conflict is not excluded in theory, but in practice we still have to see what situations in cyberspace will be considered by states as such an armed conflict.

Touching upon the problem of state practice in relation to cyber armed conflicts, it is important to note that there are concerns in the doctrine about the trajectory of such practice development. In particular, C. Droege notes: "... it remains unclear in which direction the practice of states will develop. Given the reluctance of states to recognize situations of armed conflict, especially non-international armed conflict, it can be assumed that attempts will be made to evade discussion of the existence of an armed conflict. And this is not only due to the anonymity of many attacks on computer networks and practical problems with attribution, but also due to the fact that most of the situations may not represent extreme cases of physical destruction caused by attacks on computer networks, but rather, bloodless manipulation of infrastructure at a fairly low level. States can consider such situations from the point of view of law enforcement and criminal law, and not as situations regulated by the legal system applicable to armed conflicts" [Droge C., 2014: 25–26].

Let us express our solidarity with the above concerns. However, it must be considered that without the relevant practice of states, the above problems will remain unresolved. At the same time, waiting for the moment when states finally form the relevant practice also seems to be a rather short-sighted decision. Of course, one can expect when states will finally form a practice on this issue, but there are other ways to identify the prevailing attitude of states on the issue. In particular, it is necessary that the problems of the typology of armed conflicts in cyberspace be brought up for discussion in international organizations, best of all, in the agenda of their plenary bodies, in the activities of which the prevailing practice of states can be traced. The best place to discuss this issue is the United Nations General Assembly, since all states of the world are represented there. Therefore, it is necessary that the UN General Assembly pay attention to the problem of qualifying international armed conflicts, include it in the agenda, as a result of which a corresponding resolution would be adopted. Let's hope that the UN General Assembly will pay attention to this problem.

References

Backstrom A., Henderson I. (2012) New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, vol. 94, no 886, pp. 483–514.

Brown G. (2011) Why Iran didn't admit Stuxnet was an attack. *Joint Force Quarterly*, issue 63, pp. 70–73.

Dinniss H. (2012) *Cyber Warfare and the Laws of War*. New York: Cambridge University Press. 331 p.

Döge J. (2010) Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime. *Archiv des Völkerrechts*, no 4, pp. 486–501.

Droege C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, no 886, pp. 533–578 (in Russian)

Hathaway O., Crootof R. et al. (2012) The Law of Cyber-Attack. *California Law Review*, no 4, pp. 817–885.

Lin H. (2012) Cyber conflict and international humanitarian law. *International Review of the Red Cross*, no 886, pp. 515–531.

Lin H. (2010) Offensive Cyber Operations and the Use of Force. *Journal of National Security Law and Policy*, vol. 4, pp. 63–86.

Melzer N. (2017) *International Humanitarian Law: A Comprehensive Introduction*. Moscow: ICRC. 420 p. (in Russian)

Melzer N. (2011) *Cyberwarfare and International Law*. UNIDIR Resources Paper. 38 p.

Pictet J. (ed.) (1952) *Geneva Convention (I) for the Amelioration of the Condition of the Wounded in Armies in the Field Commentary*. Geneva: ICRC. 466 p.

Roscini M. (2010) World Wide Warfare — *Jus ad bellum* and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, vol. 14, pp. 85–130.

Sassòli M., Bouvier A. (2008) How does Law protect in War? Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law. Vol. I. Outline of International Humanitarian Law. Moscow: ICRC. 672 p. (in Russian)

Schmitt M. (2019) Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, no 1, pp. 333–355.

Schmitt M. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: University Press. 598 p.

Schmitt M. (2014) Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, no 893, pp. 189–206.

Schmitt M. (2012) Classification of cyber conflict. *Journal of Conflict and Security Law*, no 2, pp. 245–260.

Schmitt M. (2002) Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, no 846, pp. 365–399 (in Russian)

Schmitt M. (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, vol. 37, pp. 885–937.

Streltsov A. A. (2014) Main development directions of the international law of armed conflicts in relation to cyberspace. *Pravo i gosudarstvo: teoriya i praktika*, no 3, pp. 75–88 (in Russian)

Sun Tzu (2016) *The Art of War*. Moscow: AST, 220 p. (in Russian)

Tsagourias N. (2012) Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, no 2, pp. 229–244.

Zhang L. (2012) A Chinese perspective on cyber war. *International Review of the Red Cross*, no 886, pp. 801–807.

On the Prospects of Digitalization of Justice

Oleg Stepanov

Chief Researcher, Centre of Criminal Law, Criminal Procedure and Judicial Practice, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Doctor of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: crim@izak.ru

Denis Pechegin

Senior Researcher, Centre of Criminal Law, Criminal Procedure and Judicial Practice, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Candidate of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: crim5@izak.ru

Maria (Dolova) Diakonova

Senior Researcher, Department of Civil Legislation and Procedure, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Candidate of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation. E-mail: civil@izak.ru

Abstract

The article considers the problem of digitalization of judicial activities in the Russian Federation and abroad. Given the fact that in the modern world elements of digital (electronic) justice are gaining widespread adoption, the article presents an analysis of its fundamental principles and distinguishes between electronic methods of ensuring procedural activity and digitalization of justice as an independent direction of transformation of public relations at the present stage. As a demonstration of the implementation of the first direction, the article presents the experience of foreign countries, Russian legislative approaches and currently being developed legislative initiatives in terms of improving the interaction of participants in the procedure through the use of information technologies. The authors come to the conclusion that the implemented approaches and proposed amendments are intended only to modernize the form of administration of justice with new opportunities to carry out the same actions (identification of persons participating in the case, notification, participation in the court session, etc.) without changing the essential characteristics of the proceedings. The second direction, related to electronic (digital) justice, is highlighted from the point of view of the prospects and risks of using artificial intelligence technologies to make legally significant decisions on the merits. At the same time, the authors argue that the digitalization of justice requires the development and implementation of the category of justice in machine-readable law, as well as special security measures of both technological and legal nature.

Keywords

digitalization, judicial activity, justice, foreign experience, artificial intelligence, justice.

For citation: Stepanov O.A., Pechegin D.A., Diakonova M.O. (2021) On the Problem of Digitalization of Justice. *Legal Issues in the Digital Age,* no 2, pp. 104–120.

DOI: 10.17323/2713-2749.2021.2.104.120

Introduction

According to the Decree of the President of Russia of May 7, 2018 No. 204 "On national goals and strategic objectives of the development of the Russian Federation for the period up to 2024", the process of digitalization of public practice is strategic in nature. The program "Digital Economy of the Russian Federation", among other things, provides for the need to improve the legal regulation of the implementation of state functions.

This trend is typical for most countries. Thus, in accordance with the Recommendations of the Committee of Ministers of the Council of Europe CM / Rec (2009) 1 on e-democracy (adopted by the Committee of Ministers on February 18, 2009 at the 1049th meeting of deputy ministers), e-justice is intended to generally improve the efficiency and quality of public services through electronic communication and data exchange; and access to judicial information.

New technologies, on the one hand, are designed to improve the life of society by simplifying access to public services, increase the efficiency of participation in economic turnover, and strengthen economic ties between actors. [Khabrieva T., Chernogor N., 2018: 85–102]. At the same time, by virtue of their technical nature, the technologies are not devoid of shortcomings, the problem modern researchers do not cease to pay attention to [Kucherov I., 2017: 69–79].

Nevertheless, the prospects for the active introduction of artificial intelligence and other digital technologies make it necessary to understand the legal regulation of these processes [Medvedev R., 2018: 14]. In this respect, justice is no exception, because its activities constitute the pivotal basis of rule of law in the state as a whole.

The range of «depth» of digitalization of the procedural form varies from the use of electronic means of communication only as a way to simplify the resolution of the case to the use of the capabilities of AI as a way to resolve the dispute itself on the merits [Povetkina N., Ledneva Yu., 2018: 46–67].

In this regard, in legal science, a distinction is made between the terms «electronic provision of justice» and «electronic justice» [Reshetnyak V., Smagina E., 2017: 16–19].

«Electronic provision of justice» consists in the use of information technology as an «auxiliary means» and is synonymous with the informatization of the court's activities. In this case, we are not talking about a complete replacement of traditional approaches with new ones — involving electronic exchange and analysis of information, but about supplementing the existing mechanisms with auxiliary ones — such as the possibility of submitting procedural documents and evidence to the court in electronic form, electronic notification, participation in court hearings via the web-conferences (without actually appearing at the courthouse), which are used exclusively with the voluntary expression of the will of the party to the dispute.

Electronic (digital) justice, on the contrary, is not limited to the use of technology as a means of simplifying the process, but involves the digitalization of justice from a substantive point of view (including by changing the subjects of the assessment of evidence and making decisions on the case). Since a process is a set of completely definite norms, rules and procedures governing the proceedings on a case, having the necessary data, it is quite possible to predict the specific outcome of any action of one or another participant in the process. Taking this feature into account would allow technical simplification and improvement of citizens' access to justice, including at the pre-trial stages of the proceedings.

In this case, the adoption of legally significant decisions is delegated to AI-technologies: for example, the evaluation by a computer of documents and evidence submitted to the court, the decision on their adoption, the issuance of final judicial acts. At the same time, electronic support of judicial activity, in contrast to electronic (digital) justice, involves the improvement of only the form of legal proceedings, without affecting its substantive part. Since the rapid development of electronic provision of justice in Russian and Western legislation cannot be fully identified with digital justice, which requires an independent model of legal implementation, it is necessary to consider the relationship between electronic provision of justice and electronic (digital) justice in more detail.

1. Electronic support for administration of justice

Both Western and Russian legislation is developing towards improving the electronic forms of administration of justice, which implies the implementation of the following main components.

1. Information transparency of judicial activity is ensured by creation of interactive search engine on the Internet, through which one can obtain information about the structure of the judicial system, the organization of the work of courts, the staff of judges, the legal basis of the activities of the courts, cases pending, etc. Such a system may provide for different levels of access depending on the status of the person: non-participant in the process, a participant in the process, a court employee. For example, in the United States, there is a service «Public Access to Court Electronic Records» (PACER), which allows users to receive information about court cases online from federal courts of appeal, district courts and commercial courts. PACER provides registered users with access to information on court cases; the use of this system is paid ($ 0.10 per page of document). The federal judicial system itself has a case management / electronic case files (CM / ECF) system, PACER is an interface to this system for public access. The system is decentralized and each court has its own servers and its own copy of the software. Each court has a live server and separate training and test servers. The test server is used to make changes and install new versions before getting started. The learning server allows users to learn how to use CM / ECF without touching real cases. Since 1997, Singapore has been operating a platform for filing documents in courts via the Internet — the Electronic Filing System.[1] The platform provides an electronic register and the entire document management system of the Supreme Court and subordinate courts. In addition, with its help, all documents submitted to the court are automatically checked for compliance with the requirements for this type of documents without involving the human factor. Further routing of the document is also designed automatically.

In Russia, there is currently no unified system of information on judicial activity: for courts of general jurisdiction there is an Internet portal GAS „Pravosudie“ (in English: Justice state information system) (www.sudrf.ru), for arbitration courts — the information system „kad.arbitr.ru“.

Further development of technical support for legal proceedings involves the creation of a single portal, which includes a card index of electronic court cases and provides interaction with other state information systems, including the «Integrated Portal of State and Municipal Services» (Rus. Gosuslugi).

2. Notification of interested parties about the course of legal proceedings, as well as interaction between the participants in the process through

[1] Available at: https://www.sicc.gov.sg/forms-and-services/electronic-filing-service (accessed: 01.04.2021)

the use of electronic means of communication. A problematic element of legal proceedings remains the notification of the persons participating in the case about the initiation of proceedings, the holding of court sessions and the performance of procedural actions. The benefits of informing the parties to the process using the Internet, in terms of speeding up and simplifying the notification process, and reducing human and material costs, are fully recognized by governments that continue to introduce information technology into administration of justice.

As a rule, the law provides for the possibility of submitting any documents to the court in electronic form, as well as the electronic exchange of documents between the parties and the court. Almost everywhere, electronic communication requires the separate consent of the participant in the process. So, in Germany, an electronic document can be sent to the parties to the proceedings if they have expressly agreed to transfer documents electronically (clause (3) §174 of the German Civil Procedure Code). Fully electronic communication is established between courts and government agencies and institutions. Secure channels for the transmission of documents have been established: through a specific e-mail; through a special electronic mailbox of a lawyer; through the mail of an authority or a legal entity of public law; through other nationwide transmission channels that guarantee the authenticity and integrity of the data.

The Civil Procedure Rules of England also establish the possibility of sending court documents by electronic means of communication (6.23 (5), 6.23 (6)). Instruction 6A detailing these rules (para 4.1- 4.3) specifies that a document can be sent by fax or other electronic means when:

the party (its representative) has previously informed in writing about its readiness to receive notifications by fax or other electronic means and has provided an e-mail address or other electronic identification;

the fax number or e-mail address is indicated on the official documents submitted by the party (its representative).

In this case, if a party intends to serve a document using electronic means (except for facsimile communication), you should first ask the other party if there are any restrictions in the recipient's consent to accept documents by such means. The legislation of the post-Soviet states — Georgia, Kazakhstan, Moldova, Ukraine, Estonia, etc. also contains a number of norms related to the digitalization of legal proceedings.

In the conditions of free will of the parties to the law enforcement process, there is an active use of information exchange between the parties

through electronic communication, which is explained by their equal interest in the prompt consideration of the case. The approach, in which electronic channels of communication are selected by the parties on their own, seems to be more correct and effective than the imposition of digital technologies by the state authorities.

The practice of electronic legal proceedings is quite widespread within the judicial systems of countries such as Austria, Denmark, Italy, Canada, the Netherlands, Saudi Arabia, Singapore, the US, Sweden, South Korea, etc. In these states, as a rule, the legislative level provides for the possibility submission of any documents to the court in electronic form, as well as the exchange of documents between the parties in electronic form. Almost everywhere, with the exception of Singapore, special consent of the party is required for electronic interaction.

According to Russian law, applications, complaints and other documents can also be submitted to the court in the form of an electronic document signed with an electronic signature or by filling out a form posted on the official website of the court. Electronic methods of notifying the participants in the process are becoming more and more widespread: for example, in the arbitration process, after receiving the initial notification in the traditional form, no subsequent notification is made — the relevant acts are posted on the portal, and the parties can independently familiarize themselves with them. In civil proceedings, such a rule so far only applies to state bodies and organizations, but in the draft laws currently being developed, it is proposed to extend such regulation to citizens.[2]

3. The use of information technology in the proceedings on the merits. Currently, in some Western countries, computer technology and electronic communications are used to better organize the work of courts, to speed up and simplify legal proceedings. To this end, an electronic case management system is being introduced into state courts, which ensures the management of information flows: electronic registration of a case, determination of information about the parties, accounting for incoming and outgoing documents, routing the progress of the case and monitoring procedural deadlines, preparing judicial statistics, ensuring communication with all participants of the process.

[2] See e.g. the draft of federal law «On Amendments to the Arbitration Procedure Code, Civil Procedure Code, Code of Administrative Procedure of the Russian Federation» in terms of ensuring the possibility of submitting documents to the court through a single Internet portal of public services, participation in court sessions via videoconferencing.

Such a platform allows to process and store documents with their registration, optimizing the process of legal proceedings as a whole. In the United States, as mentioned above, this is the Case management / Electronic case files (CM / ECF) system, which has been operating in all federal courts since 2004.

Currently, automation of certain types of legal proceedings is taking place, in which the simplest, indisputable claims for the collection of small sums of money are resolved. It seems that the automation of the process of making a legally significant decision is possible in those categories of cases where the subject of proof and evidence are predetermined, confirming facts that are important for the case, where the function of the court, in fact, is reduced to confirmation and certification. Such cases, first of all, include cases of writ proceedings. Some legal scholars do not consider the proceedings on the issuance of a writ (a court order) to be justice at all, since there is no adversarial procedural form, as such is the free discretion of the judge, an easy procedure for canceling the issued warrants is provided. Subject to filling out the form on the court's website, attaching the necessary evidence to it, the decision to issue the writ can be made by the program.

For example, in Germany there is an electronic writ proceeding, the introduction of which became possible when maintaining only a formal check of the application for the issuance of a warrant for the admissibility of the requirements. An application for the issuance of a warrant, containing all the necessary conditions and requirements, is filled out in an electronic form posted on the Internet, while the possibility of correcting mistakes is allowed. Re-examination of the application for admissibility is not required. At the same time, any attempts to introduce an AI-system by completely replacing the work of a judge in considering and resolving disputes and conflicts, assessing the evidence presented by the parties can hardly be supported.

The use of videoconferences in court hearings is a generally accepted practice in many countries. However, in common law countries, where jury trials are traditional, videoconferencing is an exceptional way of participating in a trial, since its use does not allow to establish personal contact with a participant in the trial.

It is noteworthy that the technical, in essence, issue of the form of participation in the hearing has an impact on the transformation of the process of proof, which can be demonstrated by the following example.[3]

[3] See: Rudnev V., Pechegin D. The Impact of the Leading Digital Technologies on Criminal Proceedings: A Case of Video Conferencing. 6th International Conference on social, economic, and academic leadership. 2020. DOI: 10.2991/assehr.k.200526.047.

As a general rule, in proceedings in the International Criminal Court (hereinafter — ICC), testimony is given by witnesses in person at the hearing.[4] This opens up the opportunity for the parties to publicly and openly interrogate witnesses, find out their answers to questions, present to the court an assessment of the reliability of the witness's testimony, which strengthens the adversarial principles of criminal proceedings in the ICC, and also complies with the rights of the accused under Article 67 (1) (e) of the Rome Statute.

However, pursuant to Article 69 (2) of the Rome Statute and the Rules of Procedure and Evidence, the Trial Chamber of the ICC may order that witness statements that have been recorded previously during a criminal investigation or in court proceedings be reproduced at a hearing. Such a decision can be taken when the witness is unable to testify due to illness, death, injury, age, or in other similar cases, such as a unique opportunity for investigation provided for in Article 56 of the Rome Statute. Or if the issue concerns ensuring the safety of participants in criminal proceedings in accordance with article 68 of the Rome Statute.

In particular, based on the requirements of Article 67 of the Rome Statute, the necessary level of security can be achieved during the interrogation of a witness through videoconferences using technologies to change the witness's voice and demonstrate only his silhouette. Moreover, under certain circumstances, the examination of a witness may be initiated under in camera and ex parte conditions, as indicated by Rule 88 of the Rules of Procedure and Evidence. For example, in order to establish his identity in a court session, but to prevent the possibility of possessing information about his (her) identity by any of the participants in the process.

However, the drafters of the Rome Statute also envisaged imposing on the ICC Trial Chamber the obligation in each case to reproduce the testimony of a witness in his absence, to take into account the potential risks of violation of the rights of the accused by this decision, including while observing the requirements of procedural economy. Thus, there is an obvious desire of the developers of the Rome Statute to lay as its basis the requirement to maintain a balance of interests of all participants in the criminal proceedings, as well as the parties (including the injured party), regardless of the form of organization of the proceedings. In any case, the defendant acquires the right in each such situation to express to the court his attitude

[4] Prosecutor v. Lubanga. ICC Trial Chamber Decision on the Prosecution's application for admission of four documents from the bar table pursuant to Article 64(9). 20 January 2011. ICC-01/04-01/06-2662. Para 13.

to the testimony presented, as well as to give counter-arguments in favour of his interpretation of the events. In doing so, one must also bear in mind the provisions of Article 64 (6) (b) of the Rome Statute, which provides for the right of the ICC to seek assistance from a particular state in order to ensure the appearance of a person at a court hearing[5], including through videoconferencing [6]under Article 93 (1) (b) Rome Statute [Broomhall B., 2003: 158], if the interests of the safety and comfort of the witness so require.[7]

With regard to all the ways of presenting the ICC information described above, the experience of its predecessor — the ICTY, which was the first to introduce a gradation of evidence depending on the form of presentation, is very interesting, which was a reflection of the inquisitorial model of constructing the process of proof. Thus, in the case of Prosecutor v. Tadić, the court found that the evidentiary value of the testimony presented by videoconference, although it is more significant than the written testimony, cannot be as significant as the testimony presented in the courtroom in person. This gradation was also adopted within the framework of the regulation of the proof process in the ICC as the successor of international tribunals.[8] According to the established gradation, the evidence will be assessed differently in the process of considering the case in the ICC on the merits. In other words, when resolving a case, the ICC will most likely give preference to testimony that was presented directly during the trial and, on the contrary, if there is «better» evidence, it will not justify the decision by written testimony not personally confirmed by one or another participant of the trial.

In this refraction of the structure of evidence, we can talk about the revival at the present stage of the idea of classifying evidence by their force, which was inherent in the inquisitorial form of criminal proceedings. And such regulation does not contradict internationally recognized standards

[5] Prosecutor v. Ruto et al. ICC Trial Chamber Decision on Prosecutor's Application for Witness Summonses and resulting Request for State Party Cooperation. 17 April 2014. ICC-01/09-01/11-1274-Corr2. Para 100, 193.

[6] Prosecutor v. Ruto et al. ICC Appeal Chamber Judgment on the appeals of William Samoei Ruto and Mr Joshua Arap Sang against the decision of Trial Chamber V (A) of 17 April 2014 'Decision on Prosecutor's Application for Witness Summonses and resulting Request for State Party Cooperation'. 9 October 2014. ICC-01/09-01/11-1598.

[7] Prosecutor v. Bemba. ICC Trial Chamber Public redacted decision on the 'Prosecution request to hear Witness CAR-OTP-PPPP-0036's testimony via video-link'. 3 February 2012. ICC-01/05-01/08-2101-Red2. Para 7.

[8] Prosecutor v. Tadić. ICTY Trial Chamber II Decision on the Defence Motions to Summon and Protect Defence Witnesses and on the Giving of Evidence via Video-link. 25 June 1996. Case No. IT -94-1. Para 21.

in the field of criminal proceedings, as well as the requirements of adversariality. On the contrary, the foregoing testifies in favor of the real possibility of combining adversarial and investigative principles, and at a higher level — within the framework of building a digital evidence process and organizing judicial activity.

An essentially new stage in the informatization of the administration of justice is the creation of fully electronic courts. For example, the Hangzhou Internet Court in China, established in August 2017, is one of the first courts in China to consider cases exclusively via the Internet, and it has jurisdiction over intellectual property disputes on the Internet.

The legislative initiatives currently being developed in the following areas are aimed at a wider application of the latest technologies in Russian legal proceedings: remote electronic appeal to the court through the personal account of a participant in the trial; remote receipt of subpoenas and other court notices in the personal account of the participant in the process; remote receipt of judicial acts and their copies in electronic form in the personal account of the participant in the process; the possibility of admitting persons to participate in court sessions through a web conference, without the need to appear in person in court by authenticating the participant using his biometric personal data.

It should be noted that now in Russia, electronic technologies are most actively used in the arbitration process, to a lesser extent in civil, administrative and criminal proceedings, which is largely due to the difference in the technical support of courts of general jurisdiction and arbitration courts, as well as the specifics of the participants in cases considered in these types of courts. In this regard, it seems promising to change the emphasis in legal regulation — the use of traditional means only in cases where there is no technical ability to access electronic means of communication, provided there is a voluntary consent of interested parties to electronic means of interaction.

The indicated implemented approaches and proposed innovations are intended only to modernize the form of administration of justice with new possibilities for carrying out the same actions (identification of persons participating in the case, notification, participation in the court session, etc.) without changing the essential characteristics of the proceedings.

Meanwhile, it should be borne in mind that today a new digital sphere of public relations is being formed, requiring not only the modernization of legislation, but also the adaptation of the judicial system to changing reali-

ties. Digital justice is fundamentally different from the use of information technology only to improve the form of traditional legal proceedings.

At the same time, we note that the term "digital justice" is more in line with the future vector of development of the state and society. The substantive difference of digital justice is that it will affect not only the modification of the form of legal proceedings, but also the composition of the participants in the process, the rules for assessing evidence, etc. At the same time, analyzing these transformations, it is necessary, first of all, to determine the relationship between the concepts of "digital justice" and "justness" ("fairness").

2. Problems of ensuring fairness and security of digital justice

The activities of the state related to the consideration of a case of an offense or a legal dispute determine the content of the jurisdictional function of the authorities, since justice is the most perfect means of legal protection of the interests of the state and the individual [Kuzurmanova I.V., 2011: 37–40].

Proceeding from the fact that the main function of the judiciary is to administer justice and the court is called upon to restore the right in case of violation of the law, it is important to consider such power not just as a separate part of the state mechanism, but as the power that confirms the fairness of the state organization of society [Pizzi W., 2016: 212].

Therefore, the digital transformation of the jurisdictional sphere should be aimed at ensuring trust in digital records, as well as establishing an appropriate regime for the collection and storage of digital evidence by programs. Such software solutions should take into account the peculiarities of regulating digital legal relations in legislation and fixing legal facts, which, among other things, will require the development of special rules of procedural evidence.

The digitalization of substantive legal relations lays the foundation for the transformation of the institutions of evidence, for example, in terms of mechanisms for determining the reliability, admissibility and legal force of digital evidence, methods of their assessment by the court, but achievements in the field of electronic forms of judicial proceedings, it seems, will not yet be able to solve the problems of digital evidence due to their attachment to traditional forms of evidence (electronic signature — handwritten signature, written protocol — audio and video recording, etc.). This circumstance is of key importance for ensuring the proper quality of «justice of the future», which should be associated with the increasing role of the

court in maintaining a balance between individuals, society and the state. At the same time, improving the quality of judicial acts through the use of digital technologies should be considered as a factor determining the formation of this balance. Based on this, at this stage, it is important to define the achievement of digital justice as the basis of «digital» fairness.

Justice (fairness) is a fundamental component of *jus naturalis* that belongs to a person from his birth. It defines the essence of law and is its basis [Saksonov A., 2016: 37]. The ability of law expresses the idea of fairness (law is a normatively enshrined and realized fairness) and is closely related to the very idea of justice. The great Russian jurist Anatoly Koni pointed out more than a hundred years ago justice cannot be excluded from fairness, i.e. come into conflict with this fundamental position [Isaev I.A., 1994: 51].

The use of digital technologies designed to minimize the influence of the human factor in the process of making legal decisions can have a significant impact on reducing the potential of such a contradiction. At the same time, it is important that any modern digital technology, offering a solution to the merits of the case, is able to test the entire array of previously adopted legally significant decisions, taking into account the fact that the model embedded in them corresponds to the value foundations of justice.

Modern technologies already today most accurately predict the outcome of most cases considered by the courts. Thus, the experience of some private companies that realize the potential of the latest technologies and even AI is of interest. A prime example of this is LexMachina, a predictive litigation platform owned by LexisNexis, and Thomson Reuters' Westlaw Edge platform. This is done by automatically collecting and analyzing information posted on the Internet about court proceedings, judges, lawyers, parties and the cases themselves.

There are striking examples of programs using artificial intelligence, built on deep learning technology, to predict the results of decisions of the European Court of Human Rights.[9] Having gained access to evidence in a particular case, the technologies assessed them in accordance with the specified parameters with an accuracy of verdicts of about 79% of 584 cases considered [Aletras N., Tsarapatsanis D., Preoțiuc-Pietro D., 2016: 93].

As a result of a similar American experiment, the researchers developed a special "smart" program, which was tasked with analyzing the judgments

[9] Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-judge-robot-european-court-of-human-rights-law-verdicts-artificial-intelligence-a7377351.html (accessed: 07.07.2020)

of the US Supreme Court for the period from 1816 to 2015 through specific algorithms. The program found a connection between the circumstances of cases and the decisions made on them and accurately predicted the outcome of more than 70% of the 28,000 cases considered.[10]

In France, the possibility of using robotic programs in justice was included in the agenda for reforming the national judicial system. In the first phase, this will affect more than 2.5 million cases.[11] At the same time, the introduction of digital technologies is accompanied by security measures of both technological and legal nature.

For example, France introduced criminal liability for using the results of the analysis of judicial practice, which makes it possible to predict what decision a particular judge might make in a case. Unlike the United States and the United Kingdom, where judges have accepted it as a fait accompli that AI law firms analyze their decisions down to the smallest detail and then create patterns of future behaviour, France has decided to stamp it out.[12] The new article 33 of Law No. 2019-222 of 23 March 2019 on programming and reform of justice for 2018-2022 states that no personal data concerning judges or judicial clerks can be subjected to any kind of re-use for the purpose or as a result evaluating, analyzing or predicting their actual or perceived professional practice.[13]

Also, as digital technologies are introduced, questions periodically arise about the possible falsification of information during the investigation and trial of the case. If the investigator or the judge is dishonest, it is necessary to exclude the possibility of making certain changes and additions to the electronic document, both by establishing a ban on changing the electronic information used in proving the case, and by ensuring reliable protection of digital documents from possible modification.

The philosophy of ensuring a positive balance in terms of the introduction of these technologies and the possible costs of this process should be based on minimizing the risk of substitution of electronic data. This circumstance can be considered as a guarantee of ensuring justice in law en-

[10] Available at: http://www.sciencemag.org/news/2017/05/artificial-intelligence-prevails-predicting-supreme-court-decisions (accessed: 07.07.2020)

[11] Available at: https://www.humanite.fr/reforme-belloubet-des-logiciels-la-place-des-juges-mirage-de-la-justice-predictive-654139 (accessed: 07.07.2020)

[12] Available at: https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/ (accessed: 07.07.2020)

[13] Available at: https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33 (accessed: 07.07.2020)

forcement in Russia, since the development of technologies is significantly ahead of the understanding of the moral and social consequences of their application. Therefore, one of the main tasks for modern lawyers will be to solve the problem of introducing into new systems of machine-readable law such algorithms that are able to assess the presence of a "spirit of law" (ie, ideas reflecting justice) in the text of a normative act.

For example, in 2018 the Council of Europe European Commission for the efficiency of justice (CEPEJ) for the first time adopted the document "European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" (hereinafter — the Charter), which establishes ethical principles concerning the use of AI in judicial systems and in the settlement of disputes: the principle of respect for fundamental rights; the principle of non-discrimination; the principle of quality and safety; the principle of transparency, impartiality and fairness; the principle of «under the control of the user».[14]

The development of an appropriate legal basis for the use of AI and the determination of the boundaries of automated information processing while maintaining the control of the decision by the judge, including the determination of grounds for refusing to execute it due to malfunctions, unauthorized external influences, etc., are necessary conditions to ensure the observance of human rights in the conditions for delegating the dispute resolution function to AI.

This means that already at the stage of software development, the norms prohibiting direct or indirect violations of fundamental values protected by the law of the national and international levels, including the Constitution of the Russian Federation, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international treaties should be fully integrated into domestic legislation. And given the ability of information technology to identify existing differences by grouping or classifying data pertaining to individuals or groups of individuals, the risks of replicating and exacerbating such discrimination should be prevented.

For example, Article 2 of the Charter states that discrimination can include perceived racial or ethnic origin, social origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometrics, health data, or data related to sexuality. When such discrimination is identified, consideration should be given to taking corrective measures

[14] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment adopted at the 31st plenary meeting of the CEPEJ. Strasbourg, 3-4 December 2018.

to limit or, where possible, neutralizing these risks, and to raise interested participants' awareness.

The party must be informed that the final decision is binding, while preserving the right to access to justice, so that the case can be tried directly by a judge within the meaning of Article 6 of the European Convention.

In this regard, the requirements for maintaining control on the part of the judge, creating the ability to review automated decisions and providing access to the data array used for such automated resolution of the case are especially important.

Conclusion

The future of legal regulation related to the digitalization of judicial activity involves the development of two areas that require independent assessment. The first is the development of methods to simplify and speed up legal proceedings using information technologies as an analogue of traditional judicial actions, such as electronic court notice, electronic form of evidence, electronic court case, remote participation in court hearings, etc.

The second direction in the development of justice in the digital age, possessing significant potential, at the present stage requires the solution of a whole range of tasks, primarily related to ensuring fairness and security. Digital justice is not identical to the concept of electronic support for judicial activity, since involves not just changing the form of the process, but also essentially changing it by delegating the function of administering justice to digital technologies. This circumstance, on the one hand, requires the development and implementation of the category of fairness into machine-readable law, which implies the creation of special information and analytical software systems bound by the basic values of national and international law.

On the other hand, the introduction of these technologies should be accompanied by special security measures of both technological and legal nature, in particular, by creating an appropriate legal basis for defining the boundaries of automated information processing while preserving the possibility of revising the decision made by a judge, including determining the grounds for refusing its execution due to technical malfunctions, unauthorized external influences, etc.

In other words, regardless of the form and possible software solutions, the individual should be in the center of attention of the law enforcement system. And the use of digital technologies should be considered as a tool

for achieving the goals of justice, which maximally helps to exclude the possibility of making an unjust decision in a case under the guise of compliance with the legal form.

Thus, the digitalization of justice is designed to further develop the principles of equality and adversarial processes recognized by the international community, facilitate access to justice, ensure its fairness and efficiency.

References

Aletras N., Tsarapatsanis D., Preoţiuc-Pietro D. (2016) Predicting judicial decisions of the European Court of Human Rights: a natural language processing perspective. *Peer Journal of Computer Science,* no 2, p. 93.

Broomhall B. (2003) *International Justice and the International Criminal Court: between Sovereignty and the Rule of Law*. Oxford: Berg, 215 p. (in Russian)

Dutton Y. (2012) Virtual Witness Confrontation in Criminal Cases: A Proposal to Use Videoconferencing Technology in Maritime Piracy Trials. *Vanderbilt Journal of Transnational Law,* vol. 45, pp. 1283–1294.

Isaev I.A. (1994) *A history of Russian state and law.* Moscow: Jurist, 432 p. (in Russian)

Khabrieva T.Y., Chernogor N.N. (2018) The law in the conditions of digital reality. *Zhurnal rossiyskogo prava*, no 1, pp. 85–102 (in Russian)

Khabrieva T.Y., Lebedev V.M. (2019) *Justice in modern world.* Moscow: Kontrakt, 688 p. (in Russian)

Khazhipov R.H. (1990) The role of law and morality in the implementation of the essential forces of man. Candidate of Philosophical Sciences Thesis. Ufa, 186 p. (in Russian)

Kucherov I.I. (2017) Elements of the Financial Security and its Legal Support. *Zhurnal rossiyskogo prava*, no 6, pp. 69–79 (in Russian)

Kuzurmanova I.V. (2011) Administrative activities: system decomposition. *Administrativnoe pravo i process*, no 1, pp. 37–40 (in Russian)

Livshits R.Z. (1994) *Theory of Law.* Moscow: Juridicheskaya literatura, 224 p. (in Russian)

Maksyutin M.N. (2008) *Theory of the jurisdictional process.* Moscow: Prospekt, 224 p. (in Russian)

Medvedev R.F. (2018) The problems of legal regulation of digitalization under modern conditions. *Zakonnost'*, no 9, pp. 14–15 (in Russian)

Pizzi W. (2019) *Trials without truth: why our system of criminal trials has become an expensive failure and what we need to do to rebuild it.* Moscow: Prospekt, 280 p. (in Russian)

Povetkina N.A., Ledneva Y.V. (2018) Fintekh and Redtekh: Boundaries of Legal Regulation. *Pravo. Zhurnal Vyssshey shkoly ekonomiki,* no 2, pp. 46–67 (in Russian)

Reshetnyak V.I., Smagina E.S. (2017) *Information technologies in civil proceedings (Russian and foreign experience).* Moscow: Norma, 304 p. (in Russian)

Rudnev V., Pechegin D. (2020) Impact of leading digital technologies on criminal proceedings: case of video conferencing. 6th international conference on social, economic, and academic leadership. DOI: 10.2991/assehr.k.200526.047

Saksonov A.V. (2016) Right, the art of goodness and justice. *Voprosy studencheskoi nauki,* no 1, pp. 36–38 (in Russian)

Theory of criminal procedure: competitiveness (2013) N.A. Kolokolov (ed.). Moscow: Norma, 368 p. (in Russian)

Vekhov V.B. (2008) *Fundamentals of forensic doctrine of the study and use of computer information and means of its processing.* Volgograd: University press, 404 p. (in Russian)

When Museums Go Online

Natalia Kapyrina

Associate Professor, MGIMO University, Candidate of Juridical Sciences. Address: 84 Prospekt Vernadskogo, Moscow 119454, Russian Federation. E-mail: natalia.kapyrina@gmail.com

Abstract

A report on the ICOM — UNIGE online conference "The Law & Digital Cultural Heritage Day", 11 December 2020.

Keywords

heritage, public, digitization, technologies, collections, copyright, content.

For citation: Kapyrina N.S. (2021) When museums go online. *Legal Issues in the Digital Age,* no 1, pp. 121–125.

DOI: 10.17323/2713-2749.2021.2.121.125

The coronavirus pandemic produced much sorrow and distress, but it also provided opportunities to proceed with digitization processes that had been set aside for lack of support or that had been unimaginable in previous decades. This momentum may prove particularly beneficial to such central public bodies as courts, educational institutions and museums. The acceleration of digitization, albeit with regional differences, has revealed the limits of interactions in the digital environment while also multiplying the options available and adding value to existing institutional functions and practices without replacing them, as some had feared.

Digitization of museum collections contributes to these institutions' core missions of preserving the cultural heritage, enabling research based on their collections, and disseminating knowledge.[1] In particular, digitization facilitates preventive conservation, innovations in interactive viewing,

[1] See the 2007 ICOM definition of a museum, which is currently undergoing a revision: "A museum is a non-profit, permanent institution in the service of society and its development, open to the public, which acquires, conserves, researches, communicates and exhibits the tangible and intangible heritage of humanity and its environment for the purposes of education, study and enjoyment." Available at: https://icom.museum/en/resources/standards-guidelines/museum-definition/ (accessed: 12.11.2019)

supports ongoing creativity, and provides broader access for scholars and the public to collections that are not on view. However, the turmoil from the pandemic that began in 2019 emphasized the scarcity of financial and human resources for museums while also bringing to the fore issues that museums have encountered in respecting copyright and related rights.[2]

Museums are indeed exposed to legal uncertainty concerning how intellectual property rights apply to several aspects of their activities. On the one hand, they use works protected by copyright, for which they must either obtain authorizations or else operate within the boundaries of specific or general exceptions and limitations. On the other hand, they exploit such works through licenses, legislative arrangements or related methods, such as employing databases which may touch upon works that are already in the public domain. The lack of a coherent and harmonized legal framework not only discourages some digitization processes but also restricts transnational collaborations. This shortcoming has been criticized for many years, and several solutions have been proposed for some of the issues raised.[3] Nevertheless, diverging or unclear legal rules are having a chilling effect on museums worldwide as they move toward digitization because any errors committed by these central urban institutions would be very costly for them in reputational terms, *inter alia*. This chilling effect on museums has a large impact on their operations, but it also hampers art historians and deprives the public at large.

As a contribution to global debate, these issues were recently explored by a research group that Dr. Yaniv Benhamou, Justine Ferland and Prof. Marc-André Renold headed Art Law Center of the University of Geneva (UNIGE). It resulted in a set of recommendations to policymakers and museums laid down in the Policy Paper on the Digitization of Museum Collections, which was published in December 2020[4] and presented during an outstanding webinar organized by the Art-Law Center jointly with the International Council of Museums (ICOM).[5]

---

[2] See, for example, Network of European Museums Organisations (NEMO).Final Report: Digitisation and IPR in European Museums, July 2020; NEMO, Survey on Museums and Copyright, 2015.

[3] See, for example, Canat J., Guibault L., Logeais F. Study on Copyright Limitations and Exceptions for Museums. Study prepared for the Standing Committee on Copyright and Related Rights, WIPO, SCCR/30/2/. April 2015.

[4] Available at: https://www.digitizationpolicies.com/ (accessed: 10.01.2020)

[5] Available at: https://www.digitizationpolicies.com/medias/Program_Conference_WhenMuseumsGoOnline-1.pdf / https://www.digitizationpolicies.com/when-museums-go-online/ (accessed: 10.01.2020)

The policy paper divides the most prominent issues into three categories. First, twelve proposals are directed to legislators and policymakers at large in order to enhance the legal framework and to reduce the detrimental legal insecurity which is caused by the current framework. Second, a code of conduct is provided for museum professionals who must clear authors' rights before initiating digitization. If such a code of conduct for museums were to be generally recognized as setting a standard for due diligence in digitizing collections, it would provide museums with a "safe harbor". Third, the policy paper outlines a potential resolution procedure based on a standard questionnaire for the parties involved in a dispute over intellectual property rights when museum collections are digitized.

The ICOM-UNIGE webinar offered an opportunity for Dr. Yaniv Benhamou and Justine Ferland to present this report and also prompted a discussion of the most pressing issues among legal academics, and practitioners, museum professionals and scholars in the humanities who lead projects involving digitized museum collections. The intersection of such varied backgrounds and experiences was thought-provoking, especially by showing what state-of-the-art museums and research practices involve. For instance, Prof. Sarah Kenderline described ground-breaking projects on archive remix, new participatory experiences and other ways in which technologies encourage access to the cultural heritage.

On the legal side, discussionscentered on recurrent questions about the current state of copyright and expressed frustration about the lack of progress in amending copyright rules. The paucity and inadequacy of the current exceptions and limitations were pointed out by several speakers, and in particular by Prof. Florent Thouvenin. The current EU mechanism for orphan works, which requires separately clearing rights for each individual work, is quite impractical for institutions that hold massive collections, as Prof. Lucie Guibault explained. She also underlined the uncertainty that museums have about their missions in a cross-border online environment when legislative harmonization is lacking. Prof. Guibault pointed out that collective management organizations are currently unable to respond to all the needs of museum digitization simply because their repertoires do not cover all the types of works that are in the custody of museums. As one illustration, she mentioned the Victoria and Albert Museum's current exhibition entitled "Bags: Inside Out", which displays a variety of accessories that are subject to a cumulation of various IP rights in the EU. The variety of licensing practices was addressed by several speakers, and in particular by Brigitte Vezina, who described how licensing arrangements from the Creative Commons empower museums to give wider access to their collec-

tions through its licensing arrangements. She has drawn the public's attention to the need — especially in the digital realm — to clarify and reconcile the ties that link cultural heritage to an institution that "owns" it, to the author or the copyright holder of a particular work, and to the community that "holds" this cultural heritage. From a broader perspective, Dr. Elisabeth Logeais sketched the various challenges and opportunities derived from such new technologies as 3D printing and indicated how digitization may provide some answers in restitution debates. Those debates have become more public and contentious recently, especially in the countries where deaccessioning of museum collections is prohibited by law.

Dispute resolution was another topic adressed at the conference, first, in a presentation of a typology of cases that a museum may face, by Boris Wastiau, director of the Geneva Ethnography Museum. He showed the wide range of potential and actual problems involving both copyright and also image rights, for instance when a museum visitor is captured near an object from the collection and this picture is used for communication purposes. Further insights into the types of copyright cases that come to the World Intellectual Property Organization's Alternative Dispute Resolution mechanism were provided by Ignacio de Castro. Sandra Sykora stressed the need for clear dispute settlement clauses in licensing agreements between authors and the various institutions involved in digitization of museum collections. She has also highlighted the recent revision of the Swiss Copyright Act, which entered into force on 1 April 2020 and has, *inter alia*, introduced protection for all photographs, irrespective of their individual character. This is creating additional problems for museums: license agreements with photographers taking pictures of objects in museums will have to be revised. This specific issue, which is also present in other jurisdictions, was specifically adderessed in the UNIGE policy paper by proposing that no additional copyright protection be extended to digitized materials.

At this stage, it seems important to raise policy-makers' attention, in the EU and beyond, to the issues addressed in the UNIGE policy paper and initiatives alike, coming from academia and from the civil societyThe pandemic showed the importance of cultural institutions for our societies, other recent natural disasters, looting and destruction during armed conflict, and such other tragic events as the fire in the National Museum of Brazil show how necessary it is to fund digitization projects and provide clear and simple rules for the operation of the cultural institutions that carry them out. Legal uncertainty along with other hurdles such as underfinancing has resulted a very low rate of digitization, which is currently

between 5 and 10% for museum collections worldwide. The research group that came up with that estimate describes the situation as the "tip of the iceberg". Dr. Yaniv Benhamou, Prof. Lucie Guibault, and Prof. Béatrice Joyeux-Prunel at various points in their presentations mentioned another negative effect of the prevailing uncertainty: ill-conceived copyright rules lead to distortion and biased narratives, which are particularly detrimental in the field of history in general and art history in particular. When digital content is restricted, scholars tend to concentrate only on whatever materials are accessible and omit archives of visual and material culture for which rights could not be cleared. Modern intellectual property laws are legal instruments that originated in the Enlightenment era, and they should continue to adapt in order to avoid one-sided approaches and narrowing of critical thought.

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through, efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among, academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

Legal Issues in the **DIGITAL AGE**

Authors guidelines

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length
Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title
The title should be concise and informative.

Author Details
The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract
The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords
Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References
The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes
The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.

Выпускающий редактор *В.С. Беззубцев*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*

Подписано в печать 26.07.2021. Формат 70×100/16
Усл. печ. л. 8,0.