Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Review

Review
УДК: 342
DOI:10.17323/2713-2749.2023.2.158.175

New Information Technologies and Data Security

Ludmila Konstantinovna Tereschenko[1], Olesya Evgenievna Starodubova[2], Nikita Alekseevich Nazarov [3]

[1, 2, 3] Institute of Foreign Legislation and Comparative Law under the Government of the Russian Federation,

[1] Adm2@izak.ru

[2] olesyastarodubova@gmail.ru

[3] naznikitaal@gmail.com

Abstract

The paper provides a review of the research workshop "New Information Technologies and Data Security" took place on 23 May 2023 at the Institute of Foreign Legislation and Comparative Law (ILCL). The authors reflect the keynotes of the reports made by representatives of the Institute of Legislation and Comparative Law, Kutafin Moscow State Law University, National Research University–Higher School of Economics (NRU-HSE), Moscow State Lomonosov University (MGU), Plekhanov State University of Economics, Moscow State City Pedagogical University, etc. The paper provides an insight into the legal issues under discussion: concept and meaning of data security in the current environment; development vectors of the data security institution in the context of digitization; limits of sovereignty in the information domain; international legal regulators of data security; sustainable security mechanisms in the face of contemporary challenges and threats; impact of advanced information technologies such as artificial intelligence, big data, machine-sensible right to data security; personal data security; state control and liability for violation of information law, etc.

Keywords

data security; meta verse; digital avatar; personal data; biometric personal data; cross-cutting digital technologies; Big Data; artificial intelligence; information sovereignty; technological sovereignty.

For citation: Tereschenko L.K., Starodubova O.E., Nazarov N.A. (2023) New Information Technologies and Data Security. A review. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 158–175. DOI:10.17323/2713-2749.2023.2.158.175

On May 23, 2023 the Institute of Foreign Legislation and Comparative Law hosted the research workshop "New Information Technologies and Data Security".

In opening the session, moderator **L.K. Tereschenko**, Chief Researcher, ILCL, Doctor of Juridical Sciences, Honored Lawyer of Russia, Russian Academy of Sciences expert, pointed out that the process of digitization has marked a new stage for data security as new issues and challenges resulting from new technologies and new opportunities called for a review of previous decisions, and there was a change of priorities and requirements to data security, only to solicit an adequate regulatory response.

Information technologies themselves are not something to be rebuffed. They are neutral and they open up new opportunities which can be used for a variety of purposes. This changes both the amount and content of data security. Moreover, data security of one group of subjects may not exactly coincide with that of another group in terms of meaning.

Information technologies are increasingly used to interfere in internal affairs of other countries, undermine their sovereignty and violate territorial integrity. This is destructive not only for information and public psychology but also directly impacts infrastructure facilities, banking sector and national data systems through hacker attacks, dissemination of fake information, intentionally false statements, calls for mass riots, extremist action, etc.

The emergence of new types of harmful information (trash streams and fake news etc.) with a negative impact on data security drives the problem beyond the national borders, only to give it an international, cross-border dimension. Rather than targeting data integrity, availability and confidentiality, attacks seek to destroy parts of the technological infrastructure to make it dysfunctional. The good news is that both public and private sector actors increasingly address the issues of data security.

A.V. Minbaleev, Head, Information Law and Digital Technologies Chair, Kutafin Moscow State Law University, Doctor of Juridical Sciences, pointed out to the fundamental issue of personal data security in the digital environment.

The speaker identified the following key vectors of data security:

1) A need to protect personal data in the digital environment. Users leave a great number of digital footprints in terms of statistical information useful for an analysis of actions in the Web which finally provides data on human beings. In this regard, it would be reasonable to upgrade the personal data law to specify and broaden the concept of personal data.

2) Personal data processed in large amounts constitute Big Data. However, Big Data have no protection mechanism. There is a need to improve both the Big Data law regulation and processing requirements in the digital environment. Requirements to information systems for personal data are usually stationary, only to make them inapplicable to cloud-based processing of Big Data.

3) Personal data protection needs to be adjusted to the digital context.

4) Protection of biometric personal data including genetic information in the digital environment. Formation of a biometric data monopoly. The Federal Law "On Identification and/or Authentication of Natural Persons Using Biometric Data, Amending Specific Regulations of the Russian Federation and Voiding Specific Legal Provisions of the Russian Federation" (No. 572-FZ of 29 December 2022)[1] raises a number of issues of the measures to be taken and reveals risks of data leakage. The government is pursuing a set of policies to force individuals to provide their biometric personal data. There are many questions on verification of biometric personal data by banks and other subjects supposed to feed data into the system.

5) Data protection issue in light of reliability. Right of access to reliable information, right to sharing reliable information. Problem of fakes and deep fakes. Artificial intelligence is now used to discredit public officers and celebrities and to commit frauds. Apart from amending the law, the culture of sharing reliable data needs to be promoted in society.

6) Issue of digital doubles. What is a digital avatar? What is its nature? Multiple threats including cloning. Digital avatars could be deleted and amended. This segment requires an assessment and further study.

7) Use of particular digital technologies. In a number of cases we have to use information technologies or data systems that, on the contrary, may be unavailable because of sanctions. As a result, users may be deprived of possibility to exist in the digital environment. In this case, the rights of us-

[1] Collected Laws of Russia. 2023. No. 1 (part I), Article 19.

ers are significantly restricted in violation of the principles enshrined in Federal Law No. 149-FZ "On Information, Information Technologies and Data Protection" of 27 July 2006[2].

V.N. Lopatin, Head and Research Director, Republican Research Institute of Intellectual Property, Chairman, National and Multinational Technical Committees on Standardization "Intellectual Property", Chairman, Association of Russian Lawyers, Commission on Intellectual Property, Doctor of Juridical Sciences, Professor, has identified priorities for systemic improvement of data security. In his presentation, V.N. Lopatin underlined time has come to reinvent and redefine data security priorities in the context of wider use of modern information technologies.

The data security was first identified as a segment of the national security system in 1989 when it traditionally meant protection of information, state/official secrets, specific data resources and public information systems.

The following three main categories are normally indentified in the system of data security assets:

information and data resources;

data systems;

society, individual and state.

To focus the resources at necessary points, priorities need to be defined for each group of assets.

As regards information, these include above all personal data, Big Data of an enormous autonomy, intellectual property in the context of protecting proprietary interests. The use of information technologies for protecting information and data resources.

Critical infrastructure protection issues.

One of the priorities of mass media and online media is to protect persons, society and state from the impact of misleading, fake information including the one created through the use of artificial intelligence.

The national legal system of information security relies on the principles of priority of international law. Russia was among the first to propose a convention against information warfare to be adopted by the United Na-

[2] Collected Laws of Russia, 2006, No. 31 (part 1), Article 3448.

tions. The analysis of law enforcement practices suggests that these provisions are not duly followed.

There is a need to take an inventory of the country's international treaties from the perspective of national information sovereignty. Reinventing the system of international law at the regional regulatory level. In terms of data security, there is a need in strict regulation at the regional level (BRIRC, EAEU, etc.) for all three categories. Speaking at the 11th Petersburg International Legal Forum[3], D.A. Medvedev noted, on the one hand, the importance of international law and its institutions for Russia and, on the other hand, inefficient application of international law.

Giving up the practice of creating traditional institutions of international law and establishing new regional law enforcement centers.

The speaker also stressed the major role of standards across all information segments including for the law enforcement system. Russia boasts the world's first intellectual property standards system. A system of standards to apply information technologies to data security at the national, regional and international levels is critical for future national sovereignty in information.

T.A. Polyakova, Chief Researcher, Acting Head, Information law and international data security department, Institute of State and Law, Russian Academy of Sciences, Doctor of Juridical Sciences, Professor, discussed the vectors of modern legal studies in the area of data security.

As a much wider multidisciplinary concept for both research and regulation, data security is regarded as an institution. With the Russian Federation assuming the responsibility for new constitutional provisions and security of persons, society and state as applied to the use of information technologies and digital data sharing (amended Article 71 of the Constitution)[4], a serious basis for further legal support of data security has emerged. While data security ranks fourth among the strategic priorities of national security[5], the current geopolitical environment is driving it to the forefront.

---

[3] Available at: URL: https://legalforum.info/news/itogi-xi-peterburgskogo-mezhdunarodnogo-juridicheskogo-foruma/ (accessed: 24.01.2023)

[4] Constitution Amendment Law of the Russian Federation No. 1-FKZ «On Improving Regulation of Specific Issues of the Arrangement and Functioning of Public Authorities". 14 March 2020 // Collected Laws of Russia, 2020, No. 11, Article 1416.

[5] Presidential Decree No. 400 "On the National Security Strategy of the Russian Federation". 02 July 2021 // Collected Laws of Russia, 2021, No. 27 (part II), Article 5351.

The priorities for studies in the area of data security include:

specifying the concept of "data";

system of legal principles underlying the national data security;

analysis of current challenges and threats;

international experience of legal support of data security;

conceptual approaches to the development of a system of administrative and legal measures including issues of multinational cooperation;

international data law.

A.V. Morozov, Chair, Computer Law and Data Security, Higher School of Public Administration, Moscow State University, Doctor of Juridical Sciences, Candidate of Technical Sciences, Professor, discussed the issues of developing and introducing new domestic information technologies to ensure data security for Russia.

In his report "The development vectors of the data security institution in the context of digitization", **A.A. Efremov**, Leading Researcher, ILCL, Doctor of Juridical Sciences, Associate Professor, discussed the general regulatory model of data security including its elements such as strategic planning, international and domestic regulation. The strategic planning challenges for data security include multiplicity of documents, development gap between the IT, electronic engineering industry and technological development, a need to take into account the provisions of the new foreign policy vision of the Russian Federation[6].

The international regulation of data security is fraught with issues like protection of sovereignty, regulatory models imposed by unfriendly countries and international organizations (digital neo-colonialism), the data localization dilemma and cyber-space fragmentation or advanced development, export and regulation of domestic technologies, multiplicity of platforms for regulatory development (GEG, OEWG, ITU, SCO, EAEU), future participation of Russia and EAEU partners in the Council of Europe Convention on the protection of personal data, and prospects of standardization in the area of information technologies and data security.

Domestic regulation of data security raises the issues like impact of digital economy on legal regimes applicable to data including development of a legal

[6] Presidential Decree No. 229 "On Approving the Foreign Policy Vision of the Russian Federation" 31 March 2023 // Collected Laws of Russia, 2023, No. 14, Article 2406.

regime for data, transition from papers exchange to data exchange, maintaining data security in removing legal restrictions on data sharing and storage, establishment of a universal trusted digital environment, a need in trust building mechanisms to introduce digital technologies as part of legal regulation.

N.N. Kovaleva, Head, Department of Digital Technology Law and Bio-Law, National Research University–Higher School of Economics, Doctor of Juridical Sciences, Professor, discussed issues of ensuring data security in the metaverse.

The metaverse is a new development stage of the Internet and an enormous market that, on the one hand, is rich with new opportunities for manufacturing, services and entertainment while, on the other hand, is many times more prone to possible attacks, with the risk of known data security threats on the rise along with the emergence of new ones. Children are especially vulnerable among population groups. The metaverse is focused on the use of cryptocurrencies and NFT, only to make it more dependent on hardware. With biometric security built into augmented reality devices, the confidentiality of users comes under a threat.

While the metaverse is primarily about overseas servers and technologies, a Russian metaverse needs to be created. Rich with new opportunities, the metaverse technology can drive economic growth, but data security threats — especially those affecting persons — cannot be resisted without government action. It is necessary to reform the public regulation of these technologies and encourage firms to develop domestic software.

N.V. Putilo, Head, Social Legislation Department, ILCL, Candidate of Juridical Sciences, made a point that the studies of data security in the area of public health should take into account the multiple nature (from the perspective of underlying powers and implementation mechanisms) of the constitutional right of persons to health and presence of data as an element of information environment (thing at law) both in its content and implementation mechanism. At the constitutional level, this element is represented by the right to reliable data on the status of favorable environment (Article 42 of the Constitution), prohibition to collect, store, use and share private information without consent of the person in question (Article 24), and the right to freely search for, receive, transmit, produce and share information by any lawful means (Article 29).

These provisions are specified at the level of sectoral legislation, primarily within of three institutions: public sharing data important for health;

sharing health data in specific information systems set up by the government; digital profile of the patient as a complex of private data available to a limited range of persons as a new sophisticated institution emerging relatively recently.

According to Putilo, public health protection relationships understood as a legal link between "individuals, entities and government in connection with the disease prevention (including the activities to prevent consumption of poor quality products likely to damage public health), health and medication assistance, as well as incidental relationships (for example, donorship, rehabilitation)" may be divided into two segments where data security threats are at their maximum:

organization of health care;

provision of health services.

In the health sector, the integrated public information system incorporating as necessary components a set of subsystems including those responsible for data security (personal data anonymization, data protection subsystems) has become a major tool for introducing digital health services and improving organizational relationships within Russia's health care. The efforts to find more ways to protect all information in the integrated health database should become a major vector of regulation in the three areas:

data confidentiality (to avoid unauthorized access to, copying, provision or sharing);

data integrity (to avoid unauthorized deletion or modification);

data availability (to avoid unauthorized blocking or technical availability problems and to ensure timely access).

Issues in each of the three components will threaten public health that may be damaged through actions (or inaction) by both patients themselves or other parties as a result of shortcomings of information they possess.

In her report "Legal aspects of ensuring children's data security", **N.S. Volkova**, Deputy Head, Social Legislation Department, Acting Academic Secretary in ILCL, Candidate of Juridical Sciences, discussed aspects of protecting minors in the Internet.

As a background to her report, she has cited official statistics whereby 98 percent of Russian minors aged 15-18 will go online on a daily basis, an evidence confirming that children are active actors of the information en-

vironment. The web access is closely related to the ability to receive information and exercise the right to freedom of expression as a prerequisite of other digital rights to be exercised by children (in the digital environment). Moreover, the ever evolving and progressing technologies bring forth new challenges to data security in the Internet. Children's intensive familiarization with the cyberspace, vulnerability and exposure to outside influences and media trends as well as inadequate awareness of various risks in the web can harm their personal development by predetermining destructive behavior patterns in the future. Creating a safe digital environment is thus a core objective of public policies in respect of children and teenagers.

In analyzing the underlying regulatory framework, speaker observed that it is fairly extensive and includes, apart from regulations governing general issues of data sharing and protection, special provisions like Federal Law No. 436-FZ "On Protecting Children from Information Harmful for Their Health and Development" of 29 December 2010 and a number of bylaws. The recent years have witnesses a major reform of this legislation caused by a need to reflect new challenges in the information environment including for protecting rights of minors. One of the legislative trends was a focus on preservation of values typical of the Russian mentality and on ensuring comprehensive security for children. In this regard, a special responsibility should be assumed not only by the authorities and society but also families. It is the family that lays the brickwork of reference values and ensures moral and ethical development of children. It is for this reason that the Children Data Safety Concept updated in 2023 devotes so much attention to the attitudes regarding education, something that, in the speaker's opinion, is not quite in line with the document's purpose and the subject matter of the relations it covers.

Also N.S. Volkova noted that governments have been taking more steps in recent years to protect the physical, ethical, emotional and psychological state of children following interactions in the digital environment. Many states have legalized the concepts of cyber-bullying and cyber-grooming, put into effect the mechanisms to prevent these anti-social phenomena, and introduced tougher sanctions for negative effects on life and health of minors subject to web bullying. Russia has yet no legal definition of bullying and cyber-bullying reported in non-regulatory official documents as anti-social phenomena. It is clear, however, that the right pattern of behavior, readiness and ability to resist unprovoked aggression in social media are necessary communication skills in the cyberspace to become an integral part of education and upbringing. She reiterated the need for close coop-

eration between public authorities and civil society, education institutions and parents to ensure information safety, develop uniform approaches and effective mechanisms for protecting minors in cyberspace.

S.I. Konev, Deputy Dean, Legal Department, Oil and Gas Gubkin State University, has presented a report "Public control/supervision of compliance with the personal data law".

One would be hard pressed to deny a premise of Murphy's law that progress is a substitution of one inconvenience for another. In providing personal data to various information systems (both public and corporate) we gain in time or service quality at the cost of our privacy. Moreover, different forms of threats to personal data safety are ever growing. These may be risks of technical nature resulting from malfunctioning of information systems (through both intentional fraudulent actions and unintentional actions by operators) or uncontrolled personal data sharing (well manifested in respect of interpreted data) etc. The government represented by the relevant regulator cannot but respond to the threats by establishing a set of binding requirements to safe data processing addressed to all operators of personal data regardless of their status. Moreover, the mechanisms for enforcement of control and supervision assume a risk-oriented approach and preventive measures, with the latter to anticipate control. The law provides for the following preventive measures: summarizing enforcement practices, awareness raising, warning notice, consulting, preventing visit. These measures, whatever the essence and meaning of each might be, have a dual effect. On the one hand, the Roskomnadzor reports over the last few years suggest that the number of violations of binding requirements is declining. On the other hand, news portals will regularly report massive leakages of personal data at major operators such as Yandex or Sberbank. Meanwhile, it is noteworthy that the Roskomnadzor has disregarded two forms of preventive action, namely, self-assessment and encouraging fair behavior.

S.I. Konev believes these measures, in view of the dynamics of social relationships in question, to build trust between the regulator and the control subjects by allowing the latter to impact the possible risk category is in line with the risk-oriented approach as a whole. Surely, the fair behavior criteria and self-assessment methodologies will need to be developed. New forms of prevention, streamlining of control/supervision and other measures applied by the government are hoped to minimize violations of binding requirements to personal data processing in the future to guarantee privacy in the cyberspace.

I.V. Bashlakov-Nikolayev, Chair of State and Law, The Presidential Academy (RANEPA), Candidate of Economic Sciences, Senior Lecturer, has congratulated all those present with the anniversary of the ILCL and wished further centenary of fruitful activities. In his presentation "Legal aspects of data and technological security in the process of de-cartelization of the Russian economy" he observed that, according to the social regulator, the Russian economy is teeming with cartels and collusions, only to constrain competition. In addition, there is an issue of de-cartelization.

The speaker noted that the economy of the digital age makes a difference in terms of faster exchange, including that of goods, between businesses, with new contacts and partners easier to find and new transactions faster to consummate. One example is creation in Russia of five websites under the contract system for transactions in the digital form. Meanwhile, digitization of this process has brought about new threats. Did they affect cartelization?

Admittedly, they did. As reported by criminologists and anti-trust bodies, the cyberspace accounts for more than half of all crimes. Approximately 90 percent of cartels were revealed at e-auctions, as a rule at those under the contractual system, with auction participants connected with customers through various means. Here it is possible to manipulate bids and auctions and thus affect the price to be paid by the public budget for goods to be delivered. Moreover, digitization created another vulnerability — characterized by rapid exchange and manipulation of data — related to identification and comparison of bids, and pressures to abandon a bid. In addition, such vulnerabilities use technologies of artificial intelligence and big data.

Meanwhile, digitization is not only about the negative side. In fact, the early cartels which emerged outside the national borders were identifiable only with the help of human sources. Now a "digital" cartel leaves many traces which allow to identify it: for example, a big digital cat developed by the Federal Anti-Monopoly Service have already identified 90 cartels at e-auctions. The crimes of this sort are investigated by identifying digital footprints left by "digital" cartels, location of the message sender, algorithm in use, range of the parties involved, etc. These things, according to the speaker, make it easier to reveal cartels. Further improvements and upgrading of artificial intelligence and big data will facilitate de-cartelization even more. On the other hand, this creates an institutional problem of recognizing as cartels all persons regardless of their impact on competition.

As a matter of conclusion, the speaker underlined that while digitization creates more opportunities for de-cartelization than ever before, there is an institutional issue of how to interpret the definition of cartels.

Yu.V. Truntsevsky, Head, ILCL Department of Anti-Corruption Methodology, Doctor of Juridical Sciences, made a presentation "Information technologies and anti-corruption standards".

The speaker mentioned his involvement in 2000-2010 in a study targeting students in three states: Russia, Kazakhstan and the United States. One question asked as part of the study was how much liberty — including the right to privacy — they would give away for public security. It turned out that students in Russia were almost invariably prepared to sacrifice their rights for the sake of public security. He ventured to propose that if such study were conducted now, it would yield similar results. In addition, the ILCL staff conducted an empiric study of the extent of corruption in respect of digitization in general and data security in particular. The study was focused on the issues related to tax returns since this process embraces multiple data including personal data.

While in some states of the world the institution of tax return may envisage a liability extending to criminal sanctions, Finland, listed among non-corrupted states by the Transparency International, does not require any tax return since the procedure is voluntary. In Russia, the list of those to submit tax returns has become ever longer since 2008, only to require enormous time — up to several days — to complete, with whole offices employed by managers to do the job. However, it has failed to do away with corruption. On the other hand, this process could be automated and with good reason. Recently a software allowing public servants to use public resources to complete tax returns rather than do it themselves was developed jointly with a multifunctional center for public and municipal services. In fact, a person who has to file a tax return receives a pre-completed document that the speaker proposed to call a kind of "vehicle tax". The process is as follows: a person authenticates the document upon making sure the "horsepower" in question is his.

To combat corruption, the society would thus want to collect data on people. This assumes creating a digital profile to underlie tax reporting. The argument that such profile can enable data leakage with negative implications does not hold since our personal data are already available online this way or another. In the course of his report, the speaker gave an example of how he had to send his data via various communication networks, each time at the risk of being picked up and hacked.

In his presentation "Law enforcement constitutionalism as an ideological basis of data security in the context of digitalization", **O.A. Stepanov**, Chief

Researcher, ILCL's Judicial Law Center, Doctor of Juridical Sciences, Professor, discussed a number of aspects related to personal data and digital profiles.

O.A. Stepanov underlined that data security issues are relevant to each of us. An obvious example is leakage of personal data, something that causes fraudulent telephone calls, a trend exponentially on the rise. Moreover, as Yu. Truntsevsky said, there are fears of possible data leakage from the digital profile of an individual as a whole.

Privacy protection issues are normally dealt with at the level of criminal and administrative law. Meanwhile, penalties or sanctions envisaged by the legislation do not avert violations, only to further undermine data security. Once personal data get online, they remain there. One possible solution is to establish the institution of personal digital profile at the constitutional level. In this event, a personal digital profile will be treated as a relatively independent category, with individuals able to apply technological protection measures such as hiding their e-mails, domicile, etc.

In her presentation "Constitutional law substance of personal data security", **E.E. Nikitina**, Senior Researcher, Department of Constitutional Law, ILCL, Candidate of Juridical Sciences, observed that an analysis of all data security documents applicable to an individual rather than state and society reveal that these terms are not compatible by their nature. Overall, the category of personal security is almost never discussed in jurisprudence has failed to develop the relevant concept though it should be treated as and make up a part of constitutional law. The reason is technological: the farther we move online, the more of human rights (to health, education) follow suit, as though to become information rights. There should be a theoretically different approach to personal data security. It is not solely the right to information that makes up the substance of personal data security but equally a number of other constitutional rights available to individuals.

In his report "Requirements to software development process and quality", **V.A. Edlin**, ILCL Postgraduate Student, drew attention to legal issues of software quality. Despite of some requirements to software quality, all of them are related to personal data protection. Meanwhile, software is not something that hangs up in space. These products are currently used in accounts, integrators etc. The relevant examples can include a possibility to register at a service via another service, reciprocal authentication through the use of trusted systems (Yandex, Google etc.), as well as a possibility to receive cookies in accessing a website from a third-party application supposed to track and transmit data on user actions to a third party.

Such close integration is vital for the product itself. Admittedly, the security of such a system is measured by the security of its most vulnerable component. If an element of pass-through authentication is not adequately protected, the whole system may be hacked. This requires to determine a consistent set of requirements to data systems. The software development is currently *on the loose*, with many applications being produced, sometimes to last a day. With time, such applications are supposed to match the quality of the product. Meanwhile, the practice shows that users are not concerned with quality: they want access to the content they need as soon as possible and without much ado.

In this context, regulation cannot be expected to be initiated by the private sector. Therefore, specific areas and requirements to software extending beyond personal data should be identified at the legislative level. The current trends show that there is an understanding that software is not just an outcome of intellectual activities but also a service. Thus, regulations applicable to service quality should presumably apply to the Law "On Protection of Consumer Rights". There are some examples, such as car sharing, when it happens.

In her presentation "Implementation issues of official secrecy regime in the context of digitization", **E.V. Leoshkovich,** Senior Lecturer, Saint Petersburg State University of Aerospace Instrumentation, ILCL Postgraduate Student, drew attention to the fact digitization has brought about a situation when it is no longer possible to identify a list of jobs with an access to information to be kept secret. In light of the discussed vocational standards, while a physician is under obligation to keep medical secrets, the junior staff is not. New jobs like a remote banking specialist are emerging with no obligation to keep banking secrets. He underlined the issues of personal data security should be carefully examined to develop a law on official secrets or impose an obligation on everyone to keep such information confidential.

In her report, **A.V. Kalmykova**, Senior Researcher, Administration Law and Process Department, ILCL, Candidate of Juridical Sciences, discussed issues of regulating critical data infrastructure.

In her presentation "The use of information technologies for legal regulation of culture and education", **E.A. Savchenko,** Researcher, ILCL Social Legislation Department, Candidate of Juridical Sciences, drew attention to the presentation by V.N. Lopatin who said that protecting interests of state and society is a major task of data security, with a safe digital education

environment and protection of traditional cultural and ethical values being among regulatory priorities. Culture as such is part and parcel of Russia's national security strategy[7]. Meanwhile, there is still a problem of public non-awareness of this wealth that requires advertising for social cause. Moreover, the speaker has noted that there is a need to legislatively define the concept of digital culture and digital education environment, as well as the criteria of quality content.

In his report "Security of personal data and their digital footprint", **M.M. Stepanov,** Senior Researcher, Department of Legal Theory and Multidisciplinary Studies, ILCL, Candidate of Juridical Sciences, observed that the protection of the right to privacy is critical for data security. Meanwhile, the regulation of digital footprint is sparse despite a satisfactory regulatory scope of the personal data law. In this regard, in the speaker opinion, it is necessary to regulate the relationships covering personal digital footprint for protection of information on network users and their right to privacy, and for security of such data as a whole.

In his report "Legal issues of personal data collection, processing and protection", **D.A. Basangov,** Senior Researcher, ILCL Laboratory of Legal Monitoring and Sociology of Law, Candidate of Juridical Sciences, discussed the impact of digital technologies on regulation of personal data sharing and details of personal data collection, processing and protection in achieving the public objective to form a personal digital profile. The speaker identified current issues with regard to the consent to processing of personal data, their confidentiality and protection. The problem is that there is no regulatory division between giving and withdrawing consent in respect of a part of personal data. Meanwhile, operators force the user to accept these rules in order to have access to a service. Moreover, it should be borne in mind data processing continues when the subject in question no longer uses the service, only to violate, in the speaker's view, human and civil rights and interests.

The presentation also focused on the issue of collection and processing of publicly available personal data, as well as on the impact of new technologies on personal data processing. As a matter of conclusion, speaker made proposals to have artificial intelligence more responsible for a harm caused by the violation of confidentiality of personal data.

[7] Presidential Decree No. 400 "On the National Security Strategy of the Russian Federation" dated 02 July 2021 // Collected Laws of Russia, 2021, No. 27 (part II), Article 5351.

In her report "Security of personal data in the platform economy", **T.A. Klepikova**, Lecturer, NRU-HSE, Senior Manager, Yandex Taxi, pointed out that technological development and progress have a major impact on relations between individuals, society and state across a variety of areas. IT penetration and a need for data security have affected many areas ranging from public administration to social protection. Moreover, new segments and institutions — like the platform economy — emerge in the digital economy to change the current social brickwork. In Russia, more than 15.5 million people are estimated to have some experience of employment in the platform economy[8]. Meanwhile, even more numerous are those who consume its products and services, only to require to take into account their rights and obligations, with personal data security issues in this area becoming a specific regulatory priority.

Russia's current statutory regulation follows a trajectory of protecting the integrity and sustainability of the national segment of the Internet, providing for universal identification rules, substituting for software/hardware imports, ensuring the digital sovereignty and security of critical data infrastructure. This is suggestive of a narrow and technology-oriented approach to data security.

Personal data security in the context of platform relationships will require a more general and comprehensive approach to include both organizational/technical security measures, guarantees of civil rights and liberties in the Internet, economic and public law aspects. Meanwhile it is not possible to describe the range of legal guarantees available to individuals on platforms for lack of a generally acceptable definition of the platform economy in either law or doctrine. The aspect obviously needs further examination. A complex nature of these relationships calls to apply the provisions of information, civil, administrative, constitutional, tax, labor, mass media legislation and probably some aspects of the law on protection of children from harmful content.

In his presentation "Legal uncertainties of data security in the context of automated binding decision-making in public administration", **N.A. Nazarov**, Senior Specialist, Laboratory of Regulating IT and Data Protection, ILCL, Postgraduate Student, discussed a currently urgent subject not adequately covered by the national doctrine. The sector of public administra-

[8] The Platform Employment in Russia: Scale, Motivation and Barriers to Participation: analytical report. O.V. Sinyavskaya, S.S. Biryukova et al. Moscow, 2022.

tion abounds with examples of automated binding decision-making that range from calculation of benefits, allowances and pensions to crime anticipation. Moreover, at the first glance these technologies exhibit a number of advantages for data security compared to human operator such as: artificial intelligence can avoid social engineering problems; and new systems can be developed to run automatic software tests for known cyber vulnerabilities.

Meanwhile, the use of these systems in their current shape is fraught with multiple potential risks, the first being a possibility to feed misleading information to artificial intelligence through other technologies. For example, one can clone the voice and video image of someone requesting a benefit or subsidy to be transferred to a bank account. Moreover, misleading information can be created in real time using the so-called *deep fake* technology. The second issue is possible leakage of data with serious implications for individuals, society and state. The data used in such systems is not a chaotic dataset but an already processed data array on each specific individual. The third issue is a possibility to manipulate input data. The knowledge of weights allows to manipulate data, that is, provide those documents that are more important for decision-making than others. There is also an issue of *trash* data input for machine learning. Finally, the fourth problem of automated binding decision-making in public administration is that of the impact on output data. Successful computer attacks on the systems themselves can change the whole decision-making process. Presumably, the point of change cannot be identified due to the *black box* specifics of artificial intelligence. As a possible option, speaker proposed to develop requirements to the technical, organizational and legal protection.

L.K. Tereschenko thanked all speakers for interesting reports and fruitful discussions.

The research workshop and discussions were also attended by leading experts in information law: **I. Yu. Bogdanovskaya**, Ordinary Professor, National Research University–Higher School of Economics, Editor-in Chief, *Legal Issues in the Digital Age* Journal, Doctor of Juridical Sciences; **P.P. Kabytov**, Head, Laboratory of legal regulation of information technologies and data security, ILCL, Candidate of Juridical Sciences; **A.A. Tedeev**, Professor, MSU and Shenzhen University, China; **E.K. Volchinskaya**, Chief Specialist, Legal Department, Federal Notary Chamber, Candidate of Economic Sciences; **M.S. Zhuravlev**, Lecturer, Department of Digital Technologies and Biolaw, Researcher, NRU-HSE Institute of Digital Environment Law, Candidate of Juridical Sciences; **V.A. Bozhenova**, Lecturer,