ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

Legal regulation of access to information: comparison of Russian Federation and abroad

Pruel N.A.
St. Petersburg State University
St. Petersburg, Russia
pruijel@inbox.ru

Menshikova G.A.
St. Petersburg State University
St. Petersburg, Russia
menshikova.g.a@mail.ru

Melnikov E.G.
St. Petersburg State University
St. Petersburg, Russia
emiller62@mail.ru

***Abstract* — In 2019, lawmakers made another attempt to update the Civil Code, making it adequate to modern requirements in general, civil society and the digital economy in particular. The article evaluates these amendments as insufficient. The authors of the publication analyze the history and trends in the formation of legislation governing the Internet and digital society in the United States, the European Community and the Russian Federation. We have to admit that against the backdrop of successes in the development of the Internet, laws are aimed not at accelerating them, which is indicated, including in decrees of the President of the country, but at containing them. The article highlights the general trend in the development of foreign legislation: the search for the optimum between the growth of information provided by the government about its activities and reasonable secrecy, including the confidentiality of personal data, observance of commercial and state secrets. It also analyzes the information content of the sites of government and public administration institutions in Russia.**

Keywords — Digital economy, Internet, legislative regulation, Civil Code, digital rights, cryptocurrencies.

I. INTRODUCTION

On October 1, 2019, the Russian Federation adopted amendments to the Civil Code (in the 1st, 2nd and 4th parts) introducing the concept of "*digital rights*", or rather, *digital rights*, since quotation marks are no longer used in writing. Recorded by law, they have become real bearers of property-law relations. This, of course, is a step forward on the path to digital economy implementation, but by no means as large as expected.

The definition of digital rights gives us concern. They are "recognized as binding or other rights named as such in the law, the content and implementation of which are determined in accordance with the rules of the information system that meets the attributes established by law" (the Civil Code, Ch. 6, Art. 141.1, Item 1). Perplexity arises from both the vagueness of the definition (even from the point of view of formal logic, an indication of the kind of "binding rights" cannot be considered sufficient to specify the subject of the definition), and the eternal reference "to the attributes established by law": there is no law yet, but restrictions are already being introduced. In the same vein, with reference to non-existent rules of the information system, articles are written on the exercise of rights (Item 2, Article 141.1.).

The procedure for a transaction concluded in electronic form is also not specifically described. The Code has recognized it, although the mechanism for replacing an electronic signature with "any way that makes it possible to determine the person who expressed the will" leaves room for discrepancies (Art. 160, Item 2). The remaining amendments, albeit of vast variety, were reduced to clarifying the general text of the Code relative to the introduction of new concepts. They are technical in nature and do not affect the mechanism that ensures their implementation in practice.

The introduction of a new relationship has begun, but only as an outline. Having legitimized the concepts of digital rights and digital money, the law did not introduce the terms that are accompanying and common in the laws of other countries, such as cryptocurrency, blockchain and smart contracts.

These amendments repeated the fate of the amendments introduced by the State Duma of the Russian Federation (February 2019) to the Civil Code under the influence of the Presidential Decree (No.1108 of 2008), when during their discussion in parliament the main articles that form the essence of civil rights and a new type of public relations were emasculated.

Around the same time, in particular, on May 25, 2019, the EU adopted the New General Data Protection Regulation, a document that stipulates the requirements for Internet regulation in European countries. It contains proposals, both for countries and firms, to clarify, first of all, laws on the privacy of information, i.e. new rules for personal data processing in the international IT market. At the same time, digital relations have long been legitimized, the concepts are included in the texts of basic laws, and ways are being sought to optimize freedom of information and privacy.

Can we consider the measures described in Russia as an adequate answer, both to the demands of the times and to the instruction by the President of the country regarding the need to reduce the backlog of Russian legislation from global standards? Hardly...

II. Research Methodology.

A. Approaches to the formation of legislation governing the information (digital) sector abroad

Abroad, the legislative execution of the information sector began in 1766 with the law Freedom of Press act (Sweden), which secured the rights of the media to publish materials on the activities of the Government and all its services Two decades later (in 1789), the Declaration of Personal Freedoms and Civil Rights was adopted in France. Further, the regulatory process went between two opposite directions, improving the mechanism for their optimization: the first is to develop the requirement for information transparency, and the second is to observe privacy rules including the permissibility of confidentiality of personal information, the secrecy of enterprises and state secrets.

With the formation and development of the field of digital information, these two areas have spread to it as well. The laws-recommendations "On Electronic Commerce" (USA, 1996), model act "On Electronic Signatures" (2001, UN Commission), the UN Convention "On the Use of Electronic Communications in International Treaties" (2005), "The Free Internet Act" (2012) were adopted. In parallel, certain articles of these acts monitored the requirements of information confidentiality. In different countries, the Internet, and, accordingly, the requirements for its regulation are treated fundamentally differently, see Table 1.

TABLE I. Freedom House's evaluation of degree of freedom of the Internet in the countries of the world (by the parameters as follows: 1 - status of law, 2 - obstacles to access, 3 - limits to content, 4 - violations of users right, 5 - act's total score)

Country	**1.**	**2**	**3**	**4**	**5**
Canada	Free	2	4	9	15
China	Not free	17	31	40	88
France	Free	3	6	16	25
Georgia	Free	6	6	13	25
Germany	Free	3	5	11	19
Iceland	Free	0	1	5	6
India	Partly free	13	10	20	43
Russia	Not free	12	24	31	67
Turkey	Not free	11	25	30	66
Ukraine	Partly free	19	16	20	45
USA	Free	4	4	14	22

The table developers (researchers from Freedom House), collected information on 66 countries of the world as of 2018, apart from those mentioned in the table, added Belarus, Vietnam, Venezuela, Uzbekistan, Emirates, Syria, Sudan (only 20 countries or almost 1/3) to the countries with non-free Internet, 30 – to partially free or almost half, and 16 (1/4) – to free. The study shows that the freedom of the Internet can also be considered a significant parameter of civilization, democracy of the country.

With common trends: a) to freedom of information; and b) to protection of privacy and secrecy; c) the similarity of the timing of the development of acts – the legislation governing public access to information is shaped differently in Europe and the USA. Unlike the European unified recommendation, the industry approach dominates in the United States. The country has developed:

- The Health Insurance Portability and Accountability Act – a set of standards creating to secure protected health information by regulating health providers;
- NIST 800-17 – a special publication by National Institute of Standards and Technology aimed at protecting Controlled Unclassified Information (CUI) in non-federal information system and organizations;
- The Gramm-Leach Bliley Act also known as the Financial Modernziation Act of 1999 that seeks to protect the personnel Information of consumers stored in financial institutions;
- The Federal Information Security management Act- a federal Law part of large E-Government Act of 2002 that made it a requirement to federal agencies to develop, document and implement security and protection program.

Overall, Data Protection Authorities took place in 60% of countries in 2018. Europe and Asia-Pacific are ahead of other regions in this regard, having a large majority of countries with a mature – or at least maturing – institutional framework. At least 109 countries around the world have adopted some form of data protection and privacy legislation. While 10% draft legislation and 21% have no legislation whatsoever. In accordance with the decisions of the UN (Commission on Trade – UNCTAD), the basis of the legislation proposed as compliance with 8 principles, table 2.

Researchers found out three types of regulations: direct, self and co-regulation (which can be similar to collaborative regulation between private sector and regulators). All three Types are applied to three levels: individual company, sector wide and economy in general.

Summing up, we may note the length of the process of the legislative system formation, the variety of forms and technologies of regulation, the activity of scientists in the analysis of the ongoing processes. "As a new dawn begins for privacy and security regulations, one thing remains certain: the challenges are global and every country has a stake".

TABLE II. 8 Core Data protection principles

Principle	**Its description**
Openness	Organizations must be open about their personal data based practices
Collection limitation	Collection of personal data must be limited, lawful and fair, usually with knowledge or consent
Purpose	The purpose of collection and disclosure

specification	must be specified at the time of collection.
Use limitation	Use or disclosure must be limited to specific or closely related purposes
Security	Personal data must be the subject to appropriate security safeguards
Data Quality	Personal Data must be relevant, adequate and up-to-sate
Access and correction	Data subjects must have appropriate rights to access and correct their personal data
Accountability	Data controllers must have responsibility for ensuring compliance with the data protection principles

III. RESULTS OF THE RESEARCH.

A. Features of the making of the European system of legislative regulation of the digital sector

Let us describe approaches to the formation of legislation in European countries, focusing on the institutional nature of the process, bearing in mind both the development of the legislative system and the institutions that provide it.

It can be considered the beginning of 1980, when the OECD approved “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”. This document (Guidelines) fixed in law the idea, that Individual would lose the right to information privacy, the right to decide for themselves how their data will be used, who it would be shared with, and for what purposes. The privacy principles enshrined in this document formed the basis of all national documents, including the Law of the Russian Federation “On Personal Data” (Federal Law No. 52 of July 27, 2006).

A new stage is “Data Protection Principles for 21-st century, 2013”. This document took into account 33 years of information user practice, as well as the new requirements of the time arising from the formation of the “Big - Data” information flows or “Big - Data” World. Main priorities for modernizing Guidelines, 1980 were:

- reduce the focus on data collection and focus more on practical assessment on the benefits and risks,
- restore the balance before the privacy and free flow of information,
- make data-users more accountable for the personal data they access,
- adopt the broader definition of the “harms”, that inappropriate users of personal data can cause (h.11 Data Protection Principles for 21-st century”).

Its basis was the formation of 8 mandatory principles we already described, see table 2.

To describe the next step, we will describe the activities of the European Data-Protection Supervisor Board (EDPSB). The organization has replaced the bureau of supervisors previously responsible for monitoring compliance with European legislation in the field of the digital economy. It was designed to control the activities of 66 agencies from 29 EU member states, and its mission was reflected in Regulation 45/2001, Regulation 2018/1725, which was a new milestone, formulating the tasks for EDPSB.

We will also name other documents intended to draw up legal support for digital technologies: «E -privacy regulation, 2017», «Regional report to access to information and big-data protection, 2012», «Ethic advisory group report, 2018». The huge and versatile activities of the EU were embodied not only in supervision, but also in holding conferences on various issues of coordination of efforts of countries and agencies, for example, "Debating ethics: Dignity and respect in data driven life", 2018. Several Internet platforms have been created, for example, “Internet Privacy Engineering Network (IPEN), 2018”. To carry out the work, a control center - a data-protection officer was created, its work was carried out in the framework of the developed documents "Data-protection Law enforcement Directive, 2018" and "The General data-protection regulation, GDRP, for countries of EU, 2018"

Annually they published reports reflecting the variety of forms of work of the organization, in particular “European Data-Protection Supervisor. Report 2018”. Note that this is the second report; 2018 saw the report “Data Protection and Privacy in 2017”

The reports recorded basic values: Impartiality, Integrity Transparency, Pragmatism and Guiding Principles: to serve public Interests, to use expertise, authority and formal powers, to focus attention at spheres of administration, which contain highest risks. In accordance with the strategy of the new controlling organization developed in 2015, its methods were named as follows: supervision, consultations, cooperation, collaboration, monitoring, compliance, and the main activities:

- monitoring and respecting to technical developments,
- promoting privacy engineering,
- establishing the state if art in data-protection by design.

The core of the activity was “New legislation adequate to new era”, the developers of which tried to find the optimum between observing privacy and openness, including by implementing a culture of accountability.

The monitoring was carried out both for the compliance with legislation (documents), and for individual political drives. Using networks (platforms), the feasibility of monitoring 4 processes was recognized:

1.The processing of data as part of Europe’s operational analyses project.
2. The processing of data on migrants arriving to Italy and Greece.
3. The processing of data relating to individuals in age 18 (labeled as subjects).
4. The processing of data in European informational system.

In addition, the activities of law enforcement organizations were monitored, for example, Europol, including participation in the discussion of annual work plans, the creation of information platforms on current activities, and the creation of Internet referral management application. The Internet Corporation of assigned names and numbers (ICANN) operates within EDPSB. The organization (EDPSB) coordinates the activities of national law enforcement agencies that monitor compliance with Internet laws in their countries. The Crime Information Cell portal exchanges information in a

wider field than Interpol, i.e. includes Common Security and Defense Policy, Justice and Home Affairs.

Let us outline other areas of EDPSB activity, thus demonstrating the scope of work and the diversity of applications:

- the development of the legislative system and control over its compliance with unified requirements (1), development and implementation of Guidelines for Data Protection in Companies and Agencies (2) and for cloud computing services (3).
- the development of the Legislative package of "A New Deal for Consumers", called to regard better enforcement and modernization of EU consumer protection rules and protect individuals from "systematic harms" in digital markets.
- the monitoring of the legislation implementation in countries and enterprises, implementing the methods of consultation described above, holding seminars and conferences, training specialists,

The organization has its own portal (EDPS website), designed to make the organization's activities open, to organize a communication system not only "vertically", but also horizontally, i.e. between participating countries, their enterprises. It has a special feedback option, where everyone is invited to express their opinion on the draft laws or documents under discussion (Opinion). The portal is constantly being improved in order to facilitate the search for partners and reduce the time needed to find the necessary information.

In parallel with this independent body, an advisory (general) board, the Joint Scrutiny Group, has been created at the European Parliament, it includes over 1,200 people representing both the Parliament and national governments.

Scientists note that the formation of legislative standards governing the Internet and relations in the digital economy is at its early stage. Many questions must be studied, i.e. go through practical testing or experimental verification, in particular the interaction of banks, the media and classified information. The main problem is the search for the optimum between the protection of personal rights and compliance with the requirement of transparency of information, including for combating corruption.

It is equally difficult to build a Compliance system in enterprises. There are general trends outlined within which enterprises create individual contracts. While this requirement is mandatory for all agencies, another 30 companies have voluntarily joined it. Currently, the contracts regulate: confidentiality of personal data of employees (35%), restriction of data-subjects rights (30%), right to access (20%), excessive collection (7%), discipline, change of purposes and others (2% each) (Report 2018 , p.40).

The EU shows the necessary scale of work to develop the principles of the Digital Society. It is necessary to improve the regulatory methodology, develop the practice of its implementation through training seminars and conferences, implement the principles in depth, extending not only to countries and regions, but also to enterprises, as well as their employees.

IV. Discussing the Results.

A. Informational content of sites of government and public administration institutions

Seeing the low grade of Internet freedom in the Russian Federation given by

Freedom House researchers, I would like to make it public, including by showing the inadequacy of information, for example, on the websites of government organizations. Let us recall that since 2009, the content of information is prescribed in the Federal Law-8 (in particular, in Article 13). Guidance on the requirements for the content and design of sites is contained in the Methodological document. There is a big difference between them. In order to assess the compliance of websites with legal requirements, we identified 4 groups of criteria for requirements to content: general requirements (1), those that are present in the law and absent in the methodology (2), those that were in the early version of the law, but were abolished (3), those that the authors of this work as people working with the state information would like to have (4). We will make a reservation that we evaluated the content requirements, skipping issues related to the domain name, design, content safety. Our estimates are confirmed by other studies, which note that 30% of sites do not comply with legal requirements.

To assess the content of official websites, three of them were selected: the site of the President of Russia, the site of the government of the Leningrad region and the site of the state prosecutor's office. We make a reservation right away that the first two were chosen on the basis of personal interest, the third one – in the hope of its full compliance with the professional status of the organization.

We will comment on the situation as a whole. Based on the modern understanding of the role of information, the requirements for it are constantly changing, primarily in the form of amendments to the Federal Law. In addition, the law contains an indication of the list of secret topics (Article 5) drawn up by the head of the organization, although there is a general law (UP No.90 of November 02, 2006 "On the list of information classified as state secret").

TABLE III. COMPLIANCE OF THE CONTENT OF THE SITES WITH THE REQUIREMENTS OF FZ-8 (2009).

Site Content Requirements	**1**	**2**	**3**
1. Background (general) information, including information about the organization, its rule-making activities (administrative regulations, service standards adopted in statutory and regulatory enactments), information on participation in targeted programs, texts of official speeches by management, information about work: reception hours, contact numbers, full names of responsible employees, on staffing. - statistics on the activities of the organization,	+ -	+ - available but scarce	+ no procedures for activities Hardly ever
2. Things not included in the recommended requirements, based on the text of Federal Law-8: - about the powers of state bodies, tasks and functions (Article 13, Item 3), - territorial agencies abroad (Item 4), - information about the managers (Item 5), - about the information systems that the organization possesses (Item 6), - on the established media (Item 7), - information on the public address (Item 8.1.b), - forms of citizens' applications (Item 8.1.c), - information on the protection of the population from emergencies (Item 8.1.d), - ... information on the use of budget funds (Item 8, 7, b), - ... information on benefits and deferrals to entrepreneurs (Item 8.7.,c), - about personnel, including vacancies and qualification requirements, - conditions and results of competitions (Item	+ Not found + ? ? - + - - - - ? ?	- Not found Only basic +/- ? - - - +/- - - Available and working - ? 	+ + + ? ? - + - There is a portal for communication with entrepreneurs Available and working - ?

Site Content Requirements	**1**	**2**	**3**
8.8.) - the procedure for submitting requests and responding to them (Art. 18 and Art. 19)			
3. Requirements for maintenance: - daily upgrade - publication of the enactment in 2 days	 - daily - no enactment texts	 - daily +	 daily +
4. Information from the previous revisions of Federal Law-No.8 - portal on anti-corruption activities, - a portal for reporting corruption cases, - a feedback portal, - transcripts of meetings, - information on administrative reform, - development plans - reports on their implementation, - data on state demand	 - - - - - - - -	 + + + - - - - -	 + + + - - + + -
5. additional information presented on the site	A lot of event information	There are suggestions for evaluating the activities of departments and local government	There are plans and audit reports

1 – site http://kremlin.ru/, 2 – site of Leninngrad Oblast Government (http://lenobl.ru/), 3 – site of the public prosecutor's office (https://genproc.gov.ru/).

Comparing the structure of information, one cannot fail to see a clear trend towards increased closeness, and in such important areas as anti-corruption activities of the organization, plans and reports, financial statements, statistics, general information about the activity of website visitors: their total number, the number of questions asked and answers received.

Strange as it may seem, the prosecutor's office site turned out to be the most informative, containing the registers of the planned assignments for inspections and reports on them. The website of the Government of the Leningrad Oblast has reduced the amount of information provided, but it seems to have retained an important trend – the willingness to work with the public, presenting the opportunity to evaluate the work of both departments and regional authorities. At the same time, the current version has no portal for feedback from entrepreneurs. It's a shame that the website of the President of Russia has no statistics on the country's development both economically and socially, there are no strategic plans; there is no anti-corruption plan, and our President, by law, leads this direction in the country.

V. CONCLUSIONS.

It is clear that at the moment, despite the high level of computerization of the country, the high level of training of

specialists, the system of legislative regulation of the digitalization process, which is also demonstrated by the level of amendments to the Civil Code, is far from foreign practice.

Of course, the country has general laws that regulate, on the one hand, the right of the population to have access to state information, and on the other – to keep secrecy and confidentiality of personal information. At the same time, their intensification is not happening. On the contrary, as our study on the content of websites of government agencies has shown, there is a reduction in mandatory content requirements. Based on the editions of Law No. 8, it is no longer required to provide financial information on the activities of the institution, annual reports on the work results, to have a portal on anti-corruption activities, etc.

The Civil Code has not changed the situation of protecting individual rights to privacy: banks control the financial situation of people, law enforcement agencies collect information about life and behavior uncontrollably, the rights and obligations of network providers are still unprotected. Not to mention the fact that the government's non-recognition of cryptocurrencies humiliated Russians as a nation with developed computer literacy.

References

[1] «Ob obespechenii dostupa k informatsii o deyatel'nosti gosudarstvennykh organov i organov mestnogo samoupravleniya».

[2] UP №204 ot 07.05.2018 goda «O natsional'nykh tselyakh i strategicheskikh zadachakh razvitiya RF na period do 2024 goda».European Data-protection supervisor going beyond the GDPR. Report 2018, Luxembourg, 2019, https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy_en , posl. Viewed on September 27, 2019

[3] European Data-protection supervisor, Report 2017, Luxemburg, 2018, https://edps.europa.eu/sites/edp/files/publication/ 18-03-15_annual_report_2017_en.pdf.посл. просмотр. 27.09.2019

[4] Hirsch D.D. In search of a Holy Grail: Achieving Global Privacy rules through sector-based codes of Conduct, Ohio State Law Journal, vol.74, N6, 2013, 1031-1067.

[5] http://data.europa.eu/euodp/en

[6] https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf

[7] https://web112.biz/news/6562-trebovaniya-k-saytam-gosydarstvennih-organizaciy/

[8] IYU Global ICT Regulatory Outlook, 2018.

[9] Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security, ITU, 2018, P.21, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf, posl. Viewed on September 27, 2019