ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

4/2022

Volume 3

Legal Issues in the **DIGITAL AGE**

Publisher
National Research University Higher School of Economics

4/2022

ISSUED QUARTERLY VOLUME 3

Editor's Note

Articles

Legal Issues in the **DIGITAL AGE**

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.

The journal is registered in the Federal Service of Supervision of Communications, Information Technology and Mass Media. Certification of registration of mass media серия Эл № ФС77-83367

ISSN 2713-2749

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

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Editor's Note

Research article
УДК: 340
DOI:10.17323/2713-2749.2022.4.4.13

E-Government: Legal Aspects

Irina Yurievna Bogdanovskaya

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russian Federation, ibogdanovskaya@hse.ru, ORCID: 0000-0002-6243-4301

Abstract

In the prefatory article, the author analyzes the general legal aspects of e-government. As a complex phenomenon, e-government has to be studied on the basis of multi-disciplinary approach including technical, sociological and legal. It is such approach that allows to reveal its essence. However, each multi-disciplinary approach has to be specifically developed. As regards the legal approach, it will be shaped by the changing social relationships brought about by IT technologies. The legal analysis amounts, in its turn, to the formal logical, historical and comparative legal methods. The formal logical method allows to analyze the law which supports the development of e-government. The historical method is focused at the evolution of law in the digital age. The comparative method is especially important as it allows to demonstrate the general and particular trends whereby e-government is anchored in the legislation of countries with different legal and political traditions. The paper demonstrates how e-government has absorbed the traditions of the past development when the state took a constitutional, legal and social shape. In the new context, modern legal principles — in particular, those of digital equality and technological neutrality — are sought. Their development follows a complex path, from straightforward assertion to criticism and negation, and takes a remarkably short period of time, sometimes not more than two or three decades. The Editor's note contains a summary of the documents produced by the XI International Conference "Law in the Digital Age" held with information support of the journal. The Conference featured a panel "E-Government: Legal Models in Russia and India". This issue of the journal deals with governance problems in the digital age (L.K. Tereschenko "State Regulation and Deregulation: A Case of the Communication Industry"; N.A. Danilov "The Transformation of E-Government and E-Governance in the Digital Economic Context in Russia and Elsewhere", D.A. Shevelko "Digitization in Russia: A Search for Legal Model", A.S. Lolaeva "E-Democracy: A Constitutional Dimension") and with legal aspects of platform development (N.A. Afifi, Reeta Sony A.L. "The Emergence of Online Delivery Platforms as Capital, Culture and Code: The Changing Paradigm").

Keywords

transition; law; information technologies; multidisciplinary approach; individual; society; state; public governance; constitution; digital equity; technical neutrality.

For citation: Bogdanovskaya I.Yu. (2022) E-Government: Legal Aspects. *Legal Issues in the Digital Age,* vol. 3, no. 4, pp. 4–13. DOI:10.17323/2713-2749.2022.4.4.13

Background

E-government has enjoyed an extensive development over a short recent historical period. With the starting point late in the last century, it has continued to evolve in countries with different legal culture, history and economy. As demonstrated by numerous international studies, e-government has been actively promoted in Arab States and African countries. It is thus obvious that e-government is becoming part of the civilization's overall brickwork. The question is what e-government is from a legal perspective.

E-Government: Information Technologies and Law

The development of information technologies has changed the relationships in society and finally the nature of governance by becoming the driving force of a totally new stage in its evolution. The changes affecting public administration and government machinery as well as the forms they take to interact with individuals in the postindustrial period herald a new stage in development of the state generally called *e-government*. The process of its evolution is currently visible in a majority of countries worldwide.

The ongoing processes affect a number of aspects — such as technical, social, legal — prompting a need to develop comprehensive methods of study. No single methodology will produce a full picture of e-government and its development in the world of today. This makes a case for multidisciplinary approach which will allow to appreciate e-government from various perspectives. This approach has been used recently by different agencies to construct e-government development ratings worldwide.[1]

[1] A recent example is the survey conducted by the UN. It provides the most comprehensive picture of e-government development both in the world as a whole and across

However, no integrated approach is possible unless subject-specific ones have been developed. This paper deals with a legal approach to the study of e-government.

Being a multi-faceted phenomenon, e-government is hard to be defined in a straightforward way [Chissick M., Harrington H. (eds.), 2004: 4–11]. At the early stage of its development with mainly technical issues to be addressed, e-government was largely perceived in connection with IT technologies applied to public administration, only to give an excessively technocratic flavour to the whole set of issues. The term *electronic* conventionally means new IT communication channels available to public authorities and individuals. E.V. Talapina defines e-government as a new interactive form of relationships between the parties in public administration [Talapina E.V., 2003: 248].

E-government is related not only to the Internet but also other systems which help disseminate information (call centres, cell phones, third-party network), with new concepts (mobile government, or M-government), (ubiquitous government, or u-government) emerging along the way.

Technical regulatory provisions have undoubtedly become part and parcel of e-government. The establishment of clear technical interactions of government agencies between themselves and with individuals is becoming a major condition of e-government operations. However, it would be wrong to think of e-government as being tantamount to the technology behind it.

In fact, the problem of e-government has gone beyond technical issues, once IT technologies resulted in social changes. The access to e-communication systems and services becomes a question of law as long as the society perceives it as a personal right underlying government activities. It is about the right of access to information, e-communication networks and public e-services.

Obviously, at the current stage of development, the national e-government models gradually become subject to statutory regulation as law brings social values to them. According to a just remark by D. Schartum, researcher from Canada, "ICT tools are needed to support the application

regions. See: United Nations E-Government Survey 2018. New York, 2018. Available at: publicadministration.un.org (accessed: 20.04.2021)

of legally grounded methods and to ensure proper safeguarding of legal, technological and organizational aspects" [Schartum D., 2015: 23].

E-government is emerging amid the established legal, political and cultural traditions. It is explicitly related to the assertion of digital sovereignty, something that finally contributes to the emergence of national models endowed with specific features.

E-government takes shape as the society makes a transition to postindustrial development. The underlying changes are comparable to those which affected the public administration at the stage of transition from the pre-industrial to industrial period. As a point common to both cases, the government had to assume a broader regulatory role in economic development and expand its social functions. Where the state fully or partially abandons its functions, the transformation of society is protracted, often to the point of triggering a crisis.

However, in the context of information society the government does not have to change the governance tools as drastically as at the time of transition to the postindustrial society. Its current positioning is based on what was achieved in the past: it is assumed that e-government is essentially constitutional and social at a time. Moreover, e-government is promoted through the principle of separation of powers, with all the three branches — legislative, executive, judiciary — to be developed through the use of information and communication technologies.

Since e-government is just emerging, national constitutions still lag behind the ongoing processes. The constitutional basis of e-government is established by the constitutions adopted back in the 18th (US Constitution) and in the mid-20th century (a number of European countries). However, the 21th century constitutions gradually come to include the amendments reflecting the ongoing changes.

The Constitution of Russia was amended to refer to the competence of the Russian Federation the issues of personal, societal and state security with regard to the use of information technologies and digital data transactions (Article 71, para "m").

As another example, the Constitution of Greece was amended to include the provisions on personal participation in the information society which essentially regulate new relationships between individuals and e-government despite that the latter is not explicitly mentioned. The constitution-

ally acknowledged personal right to participate in the affairs of information society is matched by the government's duty of positive action to guarantee equal and active participation of individuals in the information society.[2] The promotion of e-government for e-services and access to networks and information is thus an obligation of the state to take positive action for equal and active access to the information society for all.

The national constitutions gradually come to adopt the provision on personal data protection (Greece, Switzerland).

Thus, specific constitutional provisions emerge to govern the development of e-government, with the constitutional framework itself remaining essentially the same to ensure continuity with the previous stages of state development.

The transition to information society is actively promoted by the state which assumes the role of the IT system organizer in the public sphere. What is required from it at this stage does not amount exclusively to drafting new programmes: the environment for the development of information and communication technologies (ICT) has to be created as well.

To address the envisaged tasks, the state has to draft economic development programmes and concentrate financial resources. It is the state that determines the development of ICT, addresses the issues of standardization of technologies and of creating high-speed networks. In drafting programmes, the state should strike the right balance between technical and social issues (for example, to make sure that networks are accessible and affordable to people). In the context of information society, public access to IT technologies is a problem of major social importance. The state has to set up centres to ensure free access to ICT and Internet, as well as draft ICT-enabled education programmes.

So far countries have been searching for ways out of the current situation either by assuming the costs of public Internet access or drafting programmes for network access in public places by encouraging private investments [Holmes D., 2004: 15].

[2] "All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19". Constitution of Greece, Art. 5A.

Since the development of IT technologies requires a considerable amount of funds which cannot be fully provided from the public budget, countries define the forms of encouraging private investments. The costs serve to ensure public access to PCs including in publicly accessible facilities (post offices and libraries), create training programmes and centres for Internet literacy, with connectivity centres set up in places accessible to users. The information transparency of public authorities and provision of public e-services through the use of Internet could be improved without waiting for more users to come around, by creating a better environment, in particular, more publicly available points of access to government information resources.

Ensuring the Internet access is not only a matter of technology. This problem has a social and legal dimension of "digital equality" intrinsically related to social equality, including in terms of how the social status of different population groups is leveled off in the country. Any social inequality, including *digital inequality*, can considerably destabilize the normal functioning of society and public governance. Just as the welfare state is to guarantee social equality, e-government is to ensure digital equality, i.e. equal access of individuals to IT technologies. In the context of e-government, the access to information will depend on the share of population that can afford to use information and communication technologies [West D., 2007]. Moreover, it is obviously necessary to reduce the gap between various regions and population groups in each country regarding access to public networks and therefore to information on activities of public and municipal authorities.

Because of the social equality principle of access to government information resources and services, public authorities and local governments are obliged to use the methods of access affordable to all population groups.

Until the problem of ITC access for all is resolved, it is extremely important to provide legal guarantees of social equality in the context of information society. The principle of *digital equality* should not only be enshrined in the legislation but permeate the national law as a whole. This principle assumes the individual's right to choose how information will be made available to him — either traditionally on paper, or electronically. It is this approach that is best to ensure social equality and stability.

The development of e-government is paralleled by the formation of its legal framework, with countries drafting e-government development strat-

egies, adopting laws for security of personal data, data transactions and public data. This search for a national state model forces them both to revisit and review the traditional legal principles. Drafting new provisions is not a straightforward process. For example, the technological neutrality principle protected by law ensures the implementation of a variety of technologies. However, this is only one aspect of this principle. Its broad interpretation has stirred up the discussions of whether Internet providers should treat all users equally or may restrict the access of specific user categories. In the United States, the net neutrality was reviewed in 2017 when the Federal Communications Commission (FCC) "scrapped the so-called net neutrality regulations that prohibited broadband providers from blocking websites or charging for higher-quality service or certain content. The federal government will also no longer regulate high-speed Internet delivery as if it were a utility, like phone service".[3] Thus, the FCC revoked its the net neutrality provisions adopted in 2015, whereby Internet service providers could not discriminate against any lawful content by blocking websites or apps, slow the transmission of data based on the nature of the content, as long as it is legal, create an Internet fast lane for companies and consumers who pay premiums, and a slow lane for those who don't. Thus, while the net neutrality principle was reviewed, the issue has not been settled definitively. The search to define its content continues in other countries as well [Pitre S., 2018].[4]

Without an adequate legal framework, as was rightly observed by Russian researchers, the statutory regulation of IT penetration in executive government will be *reactive* rather than *anticipating*, with recurrent costs required for adapting the established e-government framework to long expected provisions of information and administrative law [Sokolov O.S., 2007: 32–35].

Internationally, they constitute the basis for approaches to essentially similar issues such as personal data security, interoperability, safety, access to information and sovereignty.[5]

[3] Kang C. Federal Commerce Commission Repeals Net Neutrality Rules. New York Times, 14.12.2017. Available at: https://www.nytimes.com (accessed: 26.06.2018)

[4] Available at: https://www.opengovpartnership.org/stories/net-neutrality-preserving-openness-of-government-northamerican-context (accessed: 26.06. 2018)

[5] Tallinn Declaration and the eGovernment Action Plan of 6 October 2017. Available at: https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovern-

Instead of Conclusion

The current issue of the journal deals with the role of law in regulating new institutional and functional processes in public administration and organization of the government machinery. It draws on deliberations of the panel "E-Government: Legal Models in Russia and India" held as part of the XI International Conference "Law in the Digital Age" hosted in Moscow by the National Research University Higher School of Economics.

Actual questions of the understanding of platforms, through their shared properties of infrastructure and how the lines of differentiation are blurring in urban spaces are analysed in paper "The Emergence of Online Delivery Platforms as Capital, Culture and Code: The Changing Paradigm" presented by legal scholars from India Nabil A. Afifi and Reeta Sony A.L.

E.V. Talapina in the article "The Right to Informational Self-Determination: On the Edge of Public and Private» examines the right to Informational self-determination as human right to decide when and within what limits personal data may be disclosed. The legal protection of data is based on interactions of public and private.

The paper "State Regulation and Deregulation: A Case of the Communication Industry" by L.K. Tereschenko deals with the problems of statutory regulation of the communication industry. In the current context of building a new digital economy and reducing administrative barriers, a special importance is attached to how state regulation and deregulation correlate in the communication industry. The regulation of major sectors, such as the communication industry, should be up to the challenges of today.

N.A. Danilov demonstrates the development of E-government in different culters in the article "Transformation of E-Government and E-Governance in the Digital Economic".

The problems of e-democracy and its constitutional brickwork are discussed in A.S. Lolaeva's article "E-Democracy: A Constitutional Dimension".

D.A. Shevelko explains the legal approaches trends to regulation of E-government in Russia in the article "Digitalisation in Russia: In Search for a Legal Model".

---

ment-tallinn-declaration (accessed: 16.11.2021); Berlin Declaration on Digital Society and Value-Based Digital Government of 8 December 2020. Available at: https://ec.europa.eu/isa2/sites/isa/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf (accessed:12.12.2021)

References

1. Apanasenko F.E. (2018) Prospects of E-State Promotion in Russia. *Filosophia prava*=Philosophy of Law, no. 2, p. 19 (in Russ.)

2. Chissick M., Harrington J. et al. (2004) E-Government. A Practical Guide to the Legal Issues. London: Thomson, pp. 4–11.

3. Fenwick W. et al. (2009) The Necessity of E-Government. *High Technology Law Journal,* vol. 25, no. 3.

4. Hennan P. (2010) *Governing Electronically: E-Government and Reconfiguration of Public Administration, Policy and Power.* New York: Macmillan, 389 p.

5. Holmes D. (2004) *E-Government. Strategies of E-Business for a State.* Moscow: Astrel Publishers, p. 15 (in Russ.)

6. Howard M. (2001) E-Government across the Globe: How Will "e" Change Governments? *Government Finance Review*, vol. 17, no. 4, pp. 6–9.

7. Kang C. (2017) Federal Commerce Commission Repeals Neutrality Rules. New York Times, 14.12.2017. Available at: https:www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html?mtrref=en.wikipedia.orggwp=6880C95FC8A9729Fc7D33008A13EC860gwt=pay (accessed: 26.06.2018)

8. Lolaeva A.S. (2022) Modern Information Technologies in Actions of the State Duma in Context of E-Govermnent and E-Democracy. *Konstitutcionnoe i municipalnoe pravo*=Constitutional and Municipal Law, no. 3 (in Russ.). Available at: URL: https://www.consultant.ru/law/podborki/jelektronnoegosudarstvo/ (accessed: 30.10.2022)

9. Petrova E.A., Sokolov A.F. (2018) Modernization of State Governance on the Basis of Implementing E-Government Concept. *Natcionalnye interecy*: *prioritety i bezopasnost*=National Interests: Priorities and Security, vol. 18, p. 22 (in Russ.)

10. Pitre S. (2018) Is Net Neutrality Preserving Openness of the Government in North American Context. Available at: https://www.opengovpartnership. org/stories/net-neutrality-preservong-openness-of-government- northamerican-context (accessed: 26.06.2018)

11. Schartum D. (2015) Developing E-Government Systems: Legal, Technological and Organizational Aspects. *Scandinavian Studies in Law*, vol. 4, p. 23. 12.Sokolov O.S. (2007) *Electronic State Governance.* Moscow: Jurist, pp. 32–35 (in Russ.)

13. Symonds M. (2000) Government and the Internet: The Next Revolution, *Economist*, no. 5, pp. 3–9.

14. Talapina E.V. (2003) Information Function of the State. In: Administrative and Information Law. Conditions and Prospects of Development. Moscow: Academic Legal University, p. 248 (in Russ.)

15. West D. (2007) *Digital Government: Technology and Public Sector Performance.* Princeton: University Press, 256 p.

16. Zelentcov A.B., Natroshvili G.I. (2020) Digital Maintaining of Admistrative Justice under Promotion of E-State: some theoretical issues. *Administrativnoe pravo i protcess*=Administrative Law and Process, no. 12 (in Russ.). Available at: URL: https://www.consultant.r/law/podborki/jelektronnoegosudarstvo/ (accessed: 16.05.2021)

Information about the author:

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

The article was submitted to the editorial office 14.11.2022; approved after reviewing 27.11.2022; accepted for publication 30.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Articles

Research article
УДК: 342, 347, 349. 6
DOI:10.17323/2713-2749.2022.4.14.33

The Emergence of Online Delivery Platforms as Capital, Culture and Code: The Changing Paradigm

Nabil A. Afifi

Centre for Studies in Science Policy, Jawaharlal Nehru University, ext. 136, New Mehrauli Road 110067, New Delhi, India, nabil58_sse@jnu.ac.in

Reeta Sony

Assistant Professor, Centre for Studies in Science Policy, Jawaharlal Nehru University, Flat No. 4, Godavari Hostel, Jawaharlal Nehru University, New Mehrauli Road 110067, New Delhi, India, reetasony@mail.jnu.ac.in

Abstract

The author's aims in the article are to address the understanding of platforms, through their shared properties of infrastructure and how the lines of differentiation are blurring in urban spaces. In doing so, authors of the article outline the growth of online food aggregator delivery platforms and factors that accelerated their growth. Further, the authors try to shed light on the multiplicity of algorithms by dissecting online platforms into individual algorithmic components. The disassembling of the platform improved the cognizance of various ways in which algorithms within these platforms affects the users and partners. Lastly, the authors highlight various ways and means in which online platforms are governed in urban spaces. The study finds that although both platforms and government have certain safeguards for their users and partners, but lack in strategy efforts for technological innovation under the realm of trust.

Keywords
food aggregator, algorithms, platforms, intermediary liabilities, labour law, urban spaces.

For citation: Afifi N.A., Sony R. (2022) The Emergence of Online Delivery Platforms as Capital, Culture and Code: the Changing Paradigm. *Legal Issues in the Digital Age,* vol.3, no 4, pp. 14–33. DOI:10.17323/2713-2749.2022.4.14.33

Introduction

In the past decade and more prominently after the beginning of the Covid-19 lockdown, societies have witnessed huge efforts of digitalisation, primarily in the form of digital platforms that have since mediated the urban lifestyle. The above phenomenon results in the entanglement of technology and space and also the emergence of socio-technical formations. In this sense, the platforms are often regarded as a form of urban infrastructure. As H. Mooshammer and P. Mörtenböck [Mooshammer H., Mortenbock P., 2021:12] highlight that platforms are not mere socio-technical transformations but pose the power of legal, cultural, and infrastructural change, thus opening the avenue for inquiry into the digital platforms. This paper reflects on platform urbanism in the context of the recent development in infrastructure and platform studies by focusing on food delivery platforms in India. Further, the paper illustrates various assemblages of algorithms in online food delivery platforms, which helped in mapping various contention zones between humans and algorithms. One of the major contention issues for platforms has been the intermediary or aggregator liability. Lastly, the paper presents the status of the liability in India within the realm of online food aggregator delivery platforms.

1. Methodology

The paper, in trying to understand the reign of platforms in urban spaces, used a multidisciplinary approach. The research conducted is exploratory in nature in order to clearly understand the effects and conditions of the platform economy. The study deployed critical content analysis and a literature survey as part of the research methods. The paper used secondary data as part of research sources, which included reports from national and

international organisations, journal articles, newspaper articles and court proceedings. The graphs and tables were made using the Data wrapper web application.

2. Mapping Transition: Infrastructure to Platform

In the field of STS (Science and Technology Studies) the discourse on infrastructure is primarily focused on the intertwining of social and technological structures. The rationale for infrastructure is driven by the idea of the free flow of goods, ideas, and people [Mattelart A., 1996]. The need for this free flow to continue inevitably leads to the governance of technology to lead a free life in society. With the surge in digital platforms due to the prevalent economic conditions, the debate about the effects of platformisation has been bubbling. At one end, scholars point towards the potency of these platforms towards matching the supply with demand in the situated market [Davis N., Shibulal S., 2018]. In the same time others analytics like T. Scholz [Scholz T., 2017] have highlighted the damage they cause to workers of these platforms and society. As in most of the places in the world, in India, too digital platforms have their major user base in urbanised cities. Thus, in this sense urban spaces seem to be a crucial boundary in exploring the dimension of factors that affect the development of digital platforms. The most prevalent digital platforms in the sector of transportation, rentals, food delivery and domestic work have previously been a part of the informal economy, more evident in India. From this viewpoint, digital platforms do use material infrastructure like streets, business and residential complexes, airports, etc., but also use the immaterial dimensions like culture embedded in the society to the managerial practices in their prevalent business [Davidson N., Infranca J., 2016].

The existing literature on platforms, situated in urban spaces, recognises the role of business models and data-driven entrepreneurial efforts in reimagining the infrastructure and services offered by urban cities. The scale of their expansion has made them new urban institutions (Doorn N., 2019). As Doorn et al. [Doorn N., Mas E., Bosma J., 2021] have stated that the coronavirus pandemic has changed platform-mediated work, and both the United States and Europe have seen considerable growth in food delivery services during severe lockdowns. These platforms have expanded their networks of participating restaurants, range of deliveries and carrier

fleets due to a surge in demand. Similarly, India, too, saw a true jump in the business of food delivery platforms[1]. With such interdependency on urban spaces, these platforms codify, decodify and recodify spaces continuously in order to adapt to each other's transformations. Dominant tech giants like Amazon, Google, Apple, etc. with their data harvesting and processing scale have given birth to data-driven govern mentality of cities often termed as 'smart cities' [Vanolo A., 2014: 883–898] contrasting to this the cities which emerge as the site of confrontation between high-tech companies and subaltern subjectivities which Rossi [Rossi U., 2019] terms as 'platform metropolis.'

Whereas technological development is progressing, two distinct streams of theoretical understanding developed. The first theorisation was in the form of infrastructure studies that emerged from STS and information science, and the second one was centred around media studies referred to as platform studies. Infrastructure studies developed along two themes within STS, first along the historical perspective of Large Technical Systems (LTS) where systems like electrical power grids and telephone networks were considered in the first phase as demonstrated by Bijker and Hughes, in the later stage of the phase the shipping networks were understood as internetworks or webs. The phase included scholars like Star and Bowker who discussed the phenomenology and sociology of infrastructure. In the same time their study highlights distinctive features of infrastructure such as reliability, ubiquity, invisibility, gateways, and breakdowns.

The study on digital platforms is recent, as even the digital industry adopted the term 'platform' in the mid-1990s when Microsoft referred to Windows as a platform. In the field of management and organisation studies some researchers contextualise platforms both in digital and non-digital industries. For them, platforms are more of an architecture comprising key elements like core and complementary components and an interface for modularity [Baldwin C., Woodward C., 2008: 32]. Management and organisation identify platforms as models of innovative products with applications to the digital world.

In the context of cultural studies and political economy, the analysis of platform design and architecture is complemented by the stress on user

[1] Available at: https/www.forbesindia.com/article/brand/connect –food-delivery-sector-sees-a–huge-rise-in-orders-as-a-result-of- covid-19/61/305/1 (accessed: 20.04.2020)

agency that is majorly characterised by economic and legal implications. Thus, scholars like José van Dijck define a platform as a "set of relations that constantly needs to be performed" with users' expressions on one side and platforms' profit aims at the other side [Dijck van J., 2013: 26]. This explanation of platforms is shared by various scholars who highlight that economic interest affects the design decisions of these platforms and not merely provides users with a means to express themselves but also enables and benefits from ranking, recommendations, and analytics [Langlois G., Elmer G., 2013].

On the other front, T. Gillespie points towards the tension between agency and architecture in platforms by analysing how legal structure and technical affordances of intermediaries shape the discourse [Gillespie T., 2010].

Scholars like J. Plantin et al. [Plantin J., Lagoze C., Edwards P., 2016] have stressed that the difference in infrastructure and platforms is merely analytical and some platforms like Google or Amazon have vantaged to the point where they resemble more like infrastructure due to their ubiquitous and common nature. Currently, in a neoliberal world, infrastructure has shown similar features as platforms due to an increase in privatisation efforts and reduction of governance as a function of the market. Thus, infrastructure and platform have converged to a point where 'platformisation of infrastructure' and 'infrastructuralisation of platforms' both are possible.

Using the concept established by J. Plantin and his collaborators, they explored the difference between infrastructure and platforms. They initially focused on the 'system builders' which is central to the idea of LTS in the STS field and 'platform builders.' Although the latter seems to be the extension of the former, the key difference is in the approach, where platform builders do not strategise through vertical integration.

Thus, platforms are designed to be amplified from outside by other actors, who endure certain rules. Platforms like Windows by Microsoft, macOS by Apple or ChromeOS by Google have thrived by appealing to individual actors (like application developers in this case) to contribute to their ecosystem, rather than innovating their own standalone products. While users benefit from the standardised platform interface, independent actors utilise the code base, large consumer base and marketing power the platforms offer. Platform builders also leverage the lock-in of both the users

and independent actors, which has revenue benefits too. As the previous studies on platforms have highlighted this approach leads to various types of restrictions, updates offered by platforms, functionality, and design. In the end, attaining lock-in is the main motive of the platform builders and to suppress the construction of gateways as infrastructure studies also highlight the same effect.

Table 1

Properties of infrastructure and platform

Property	Infrastructure	Platform
Structure	De-centralised	Centralised
Component interaction	Interoperability by standardizing	Application programming interface (APIs)
Interest	Essential services	User benefits
Value	Public	Private
Scale	Large	Small-medium
Capital	Government, PPP, pay per use	Venture capital, subscription, pay per use
Sustainability	Long term	Short (frequent updates))
User Agency	Opt-in	Opt-out

Even with the argument that recently the boundary between infrastructure and platforms is diminishing, Table 1 describes the distinct features and where they overlap. In this case of platforms, the focus was restricted to food delivery platforms. Most of the properties were adopted from the study by Plantin et al.

3. The Regime of Platforms

3.1. Contextualising Platforms

Digital platforms, with all the dissonance around them about platform capitalism, the gig economy etc. have lately been regarded as the conceptual framework for analysing and contemplating social, economic and spatial developments. However, their historical and geographical embeddedness is often unnoticed (Ecker U., Strüver A., 2022). Similarly, less focus has been on the management and cultural perspectives of digital platforms. In this section, the paper focuses on what has given rise to the platform economy

in the context of online food delivery. Secondly, the section also showcases the multiple layers that accumulate to form online food delivery platforms. The multiple interactions with various algorithms within the platforms also generate liability conflicts

In highlighting these discourses, the paper also touched upon the different management practices of online food delivery platforms and the nature of the shifting cultural context.

In the above section, the study focused on the blurring line between infrastructure and platform studies. Now, it is important to understand what contextualises something as a platform. Nick Srnicek [Srnicek N., 2017: 43] in his research *Platform Capitalism* defines a platform as "a digital infrastructure that enables two or more groups to interact." Primarily, platforms act as intermediaries and collect, analyse, and capitalise on data. A prevailing characteristic of online platforms is the attainment of a self-enforcing monopolist effect and interdependency between sector platforms and infrastructures [Poell T., Waal M. et al., 2018]. As seen in the case of online food delivery platforms which depend on various online payment platforms (sector platforms) and market themselves on infrastructural networks such as Google and Facebook. This behaviour of platforms highlights their inherent tendency of converging towards the centralisation of various efforts [Guyer J., 2016]. To be within the contextual boundary of the study, the paper specifically addresses the lean platforms in urban spaces. Lean platforms prominently focus on individual services (delivery, cleaning, etc.) while following growth-oriented methods rather than profit-based strategies. An important feature of lean platforms is their reliance on maximum out-sourcing in order to operate with a fixed capital [Srnicek N., 2017: 76].

4. Rise of Online Food Delivery

Platform economies emerged as the product of technological innovation in infrastructural capabilities and the Internet. The monetary policy following the impact of the 2008 economic crash, with the inflow of capital through venture capitalist firms [Card J., 2017] into the rising entrepreneurial efforts paved the way for digital platforms.

In the case of India, the Information Technology (IT) sector generated twice more in 2010 as in 2005, thus providing confidence in the post-2008 crash economy. The number of GICs (Global In-house Centres) also

surged during the same time period. Although, the growth of online food services in India surged after 2016 and will reach the $12.8 billion mark by 2025[2] ("India's Online Food Services Have Plenty of Room to Grow," 2021). Figure 1 shows the growth trajectory of online food services in India. Till 2018, India had two unicorns, Zomato and Swiggy, in the online food delivery sector. P. Jalote and P. Natarajan [Lalote P., Natarajan P., 2019] also observed that the growth of the IT sector was the result of minimal government intervention coupled with incentive policies, a focus of the industry on skilling and development, and a high focus on process orientation, industrial collaborations and scale and entrepreneurship. Most of these factors also have a meteoric role in the rise of the platform economy in India. Currently, India is third in online food delivery business led by China followed by the United States [Reeves S., 2019].

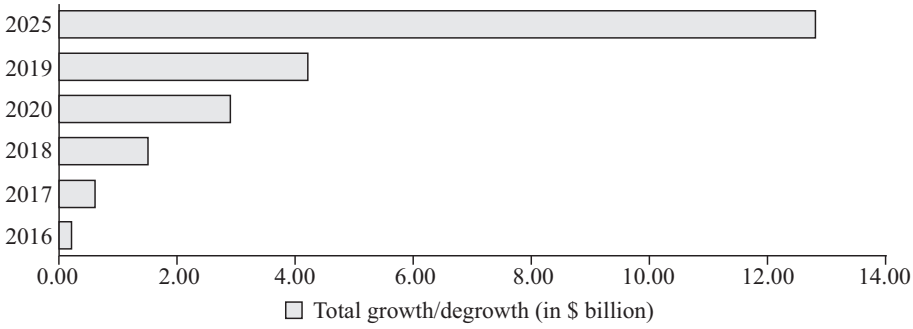

Fig. 1. Growth of online food services in India (Source: Redseer report)

Another technique to understand the penetration of online food delivery platforms is to analyse their popularity in a region. Figure 2 underlines the interest over time[3] for the term "online food delivery" in India and the rise in interest activity for the term during the beginning of the first and second phases of Covid-19 lockdowns (2020 and 2021). The interest activity also highlights the gradual rise in the popularity of the term since the mid of 2014.

[2] India's online food services have plenty of room to grow (2021, October 7). *The Economic Times*. Available at: https://economictimes.indiatimes.com/tech/startups/indias-online-food-services-have-plenty-of-room-to-grow/articleshow/86842016.cms?from=mdr (accessed: 21.04.2022)

[3] Numbers represent search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means that there was not enough data for this term. For more information visit: Google Trends

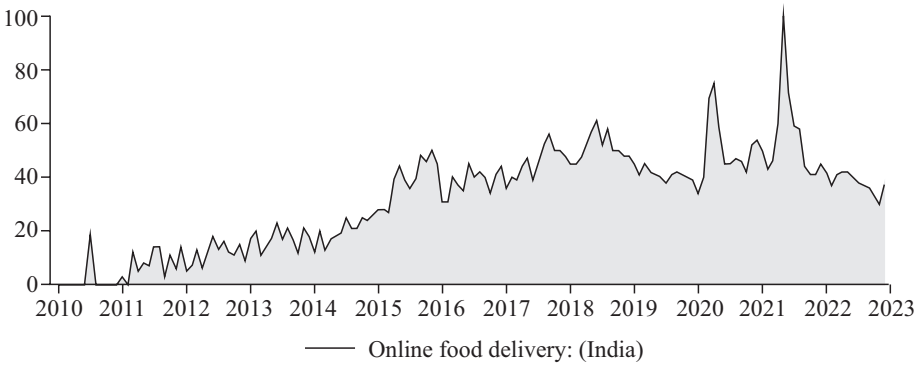

Fig. 2. Interest over time for online food delivery.

A comparison between food services in India, the United States and China put the spotlight on the existing societal practice and market penetration of food services. Indian food services market is growing but is severely underpenetrated as compared to the US and China. China dominates in food services sales with 57.8% and but the US is the leader in terms of the size of the food economy with $1780 billion. Figure 3 shows the tabular representation of food services in India, the US and China.

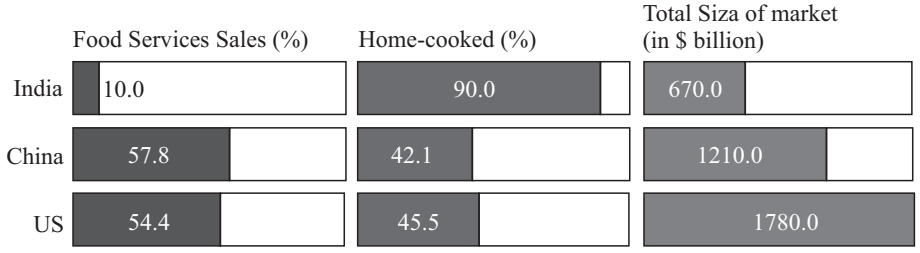

Fig. 3. Food Services: India vs US vs China (Source: Redseer report)

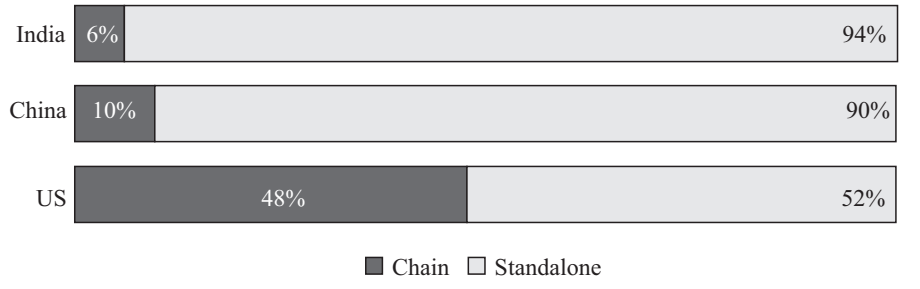

Fig. 4. Food services: Chain vs Standalone (Source: Redseer report)

Further, the Indian food market is dominated by standalone restaurants and kitchens whereas the US market although dominated by standalone restaurants, has a roughly equal percentage of food chains. Figure 4. shows the market dominance of chains and standalone restaurants in India, the US and China.

5. Dissecting Online Food Delivery Platform

Platforms are foremost an assemblage of algorithms working in a scrupulous and veiled manner. To ameliorate our conception of online food delivery platforms, it is crucial to understand the various layer of algorithms which amalgamate to form a platform. Computer scientist idea of an algorithm has predominantly been based on them being mere instructions that when executed result in the accomplishment of a singular goal. This restricted understanding considers algorithms as textual and singular in action and separates them from their technological execution. Thus, scholars in the field of algorithmic studies stress on understanding algorithms in and as action [Devendorf L., Goodman E., 2014]. Computational algorithms in action largely depend on the outside actors for data required as input, machines that execute them, the data centres that maintain results, etc. Thus, algorithms themselves are an agglomeration of public, machine, data, policies and as of any other component that may emerge over time. As Annemarie Mol [Mol A., 2002: 18] states: "It is possible to refrain from understanding objects as the central points of focus of different people's perspectives. It is possible to understand them instead as things manipulated in practice. If we do this—if instead of bracketing the practices in which objects are handled, we foreground them—this has far-reaching effects. Reality multiplies." In this context, the online food delivery platform was mapped to understand the multiple algorithms.

Figure 5 highlights algorithms in action in online food aggregator delivery platforms in India. The diagram outlines the various site of human algorithm interaction. All the terms written in white denote algorithms or algorithmic action and terms written in black are human or human-to-human interactions. This points out the areas of contention between humans and algorithms. Further, it assists in mapping the stakeholders are affected by the platformisation of urban spaces.

The inner functioning of various clusters of algorithms within the food delivery platform the multiplicity of algorithms and how different set of algorithms interact in unique ways with the users of the platform.

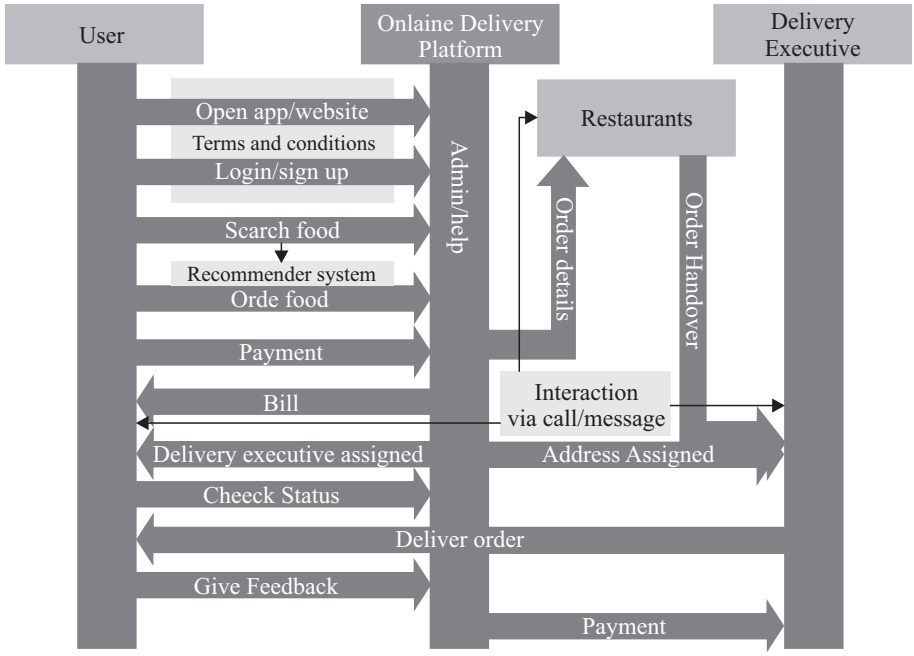

Fig. 5. Diagram of algorithms in action in an online food aggregator delivery platform

The obscurity in the functioning of these algorithms and the involvement of large user informational datasets make platforms eligible for scrutiny, although various sites for scrutiny exist within the platform. The paper focuses on the intermediary liability of online food delivery aggregator platforms.

6. Intermediary Liability of Online Food Delivery Aggregators

Platforms scale up their operations and visibility through intensive and extensive data aggregation, production and using analytics thus connecting them to existing infrastructure [Chan C., Klareld A.-S., 2022]. With the boost in the platform economy, platforms have acquired certain infrastructural properties like scale, and moreover, platforms also portray themselves as neutral, with clear boundaries just acting as mediators between different set users, strategically divesting their platform owner's power. The invisibility of LTS in our life, whereas is present everywhere is also shared by platforms as they get entrenched in our lives. For example, Zomato as a

platform work to be absent while having a nexus of delivery in the city. This strategic act reduces the role of platforms as matchmakers, although their algorithms are acting in a far more complex manner by impacting the decision-making of users [Pujadas P., Curto-Millet D., 2019].

The above argument about the power that platforms yield to users requires scrutiny from their liability perspective and what safeguards government institutions provide users within the realm of digital evolution.

Much of the population interacts with the Internet through online intermediaries; this way includes Internet service providers (ISPs), search engines and various types of platforms. The companies working in these sectors play a crucial role in providing access to information for decision-making, connecting users to other users and acting as vital drivers of economic and innovation growth. Thus, the policies embraced by these intermediaries to exercise control over users significantly shape the user's economic, social, and political selves. These policies have an implication for users' rights, expression, freedom, and privacy that are fundamental in nature in the Indian constitution.

7. Governance of Digital Platforms in India

The international legal fraternity and governments have considered an intermediary liability since their existence. A few approaches have been deployed for their governance of responsibilities and liabilities. One of the major steps towards this approach was a set of documents launched in 2015 by a coalition of Internet rights activists and civil societies. This document came to be known as Manila Principles, whose prime objective was to foster the development of interoperable and harmonised liability, which will promote innovation, amidst keeping users right at the forefront[4].

Countries like China hold intermediaries to strict liability for user-generated content, while European Union and the United States grant them leverage in form of conditional liability. Conditional liability shields intermediaries from unlawful user-generated content if they adhere to certain specific conditions as mentioned under relevant laws.

[4] Manila Principles on Intermediary Liability. 2015. Available at: https://manilaprinciples.0rg./index.html (accessed: 16.04.2020)

In the case of India, the Information Technology Act was notified in 2000, which primarily dealt with cyber-crimes and e-commerce. The amendment of IT Act-2000 in 2008 and the introduction of Intermediaries Guidelines Rules in 2011 had added certain due-diligence prospects in relation to intermediaries, which intermediaries must adopt in order to have a shelter of immunity. In the beginning, the Act was ambiguous in nature that was rectified after the important judgement in the case of Shreya Singhal v. Union of India by the Supreme Court of India in 2015 (*Shreya Singhal vs U.O.I 24 March, 2015*).[5] After which, in 2018, the Ministry of Electronics and Information Technology issued the proposal to revise the 2011 Rules. Section 2(1) (w) under the IT Act defines intermediary in detail as "Intermediary, concerning any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, on- line-market places and cyber cafes." Then under section 79 of the same act also have safe-harbour protection for intermediaries for third-party content. The function-based approach opted by the government provided safeguards to the intermediary based on the following conditions: "Firstly, observance of due diligence and certain guidelines issued by the Central Government; secondly, not conspiring, abetting, aiding or inducing the commission of the unlawful act; and lastly, upon receiving 'actual knowledge or being notified by the government, taking down unlawful content". The above safeguarding notions are provided through the provision of government-enacted IT laws, although there are other instruments also to prevent intermediaries from wrongdoings.

With the boom in the platform economy, the fair competition aspect of online platforms has also come under scrutiny that is enforced by the Competition Commission of India. Recently, a complaint was against Zomato and Swiggy (online food aggregator delivery platforms) by the National Restaurant Association of India (NRAI) for subscribing to anti-competitive practices and abuse of position by dominance[6]. The NRAI raised the is-

[5] *Shreya Singhal vs U.O.I on 24 March, 2015*. Indian Kanoon. Retrieved December 7, 2022. Available at: https://indiankanoon.org/doc/110813550/ (accessed: 20.04.2020)

[6] Available at: https://nrai.org./nrai-reaches-out-to-cci-against-anti-competitive-practices-by-zomato-swiggy (accessed: 20.04.2020)

sue of the practice of deep discounts strategies, charging high commissions from restaurants, not sharing customer data with restaurants, bundling of services, violating platform neutrality and transparency disclosures for delivery prices and commission share (ranges from 25% to 35%). The delivery partners and restaurants function through vertical integration of supply chains at various levels. But in the case of Zomato and Swiggy which are online platforms and function both as marketplace partners and competitors. The food recommender system utilised by these platforms in searching for food and price comparison generates massive traffic and user data. So, it becomes important for sellers to be listed on these intermediary platforms for business visibility and increased sales. As a consequence, these aspects make businesses depend on these platforms to access last-mile connectivity, which contributes to yielding higher bargaining power for online platforms.

Although the case is to be decided still, the Supreme Court of India judgement in the case of Uber India Systems Pvt. Ltd. v. CCI in 2019 pointed out that predatory pricing by a platform is indicative of dominance and abuse [Nariman F., 2019]. Thus, such judgements might force more regulations on online platforms. Other charges filed by NRAI can be looked at in terms of various sections under the Competition Act 2002. The deep discounts offered by these platforms come under price squeeze which under section 4(2) (a) (ii) is discriminatory and unfair in nature. The overall effect of such practices by food aggregator delivery platforms leads to a competitive disadvantage to standalone restaurants in reaching consumers of their products.

The rise of food delivery platforms has also given rise to precarious work [Iqubbal A., 2021]. The lack of employment opportunities and shifting economic conditions is one of the reasons for participating in the platform economy ("Unemployment Rate at Four-Decade High of 6.1% in 2017–2018: NSSO Surveys," 2019; "NITI Aayog Tries to Counter Bleak Unemployment Data, Says Ola & Uber Helped Create Over 2 million Jobs," 2019)[7]. Although, these online platforms create jobs which is evident by theirs success, the quality of livelihood offered needs urgent scrutiny.

[7] Unemployment rate at four-decade high of 6.1% in 2017-18: NSSO surveys. *Business Standard*. 2019, January 31. Available at: https://www.business-standard.com/article/economy-policy/unemployment-rate-at-five-decade-high-of-6-1-in-2017-18-nsso-survey-119013100053_1.html (accessed: 20.05.2021).

The International Labour Organisation (ILO) introduced a concept of 'decent work' which maintains that "the freedom to express their concerns, organise and participate in decisions that affect their working lives" of workers is fundamental [Ghai D., 2003]. According to the Fairwork report on labour standards in the platform economy in India highlights that food aggregator delivery platforms are not holding fair conditions in terms of pay, working conditions, contracts, management, and representation[8].

The labour workforce in India is supported through labour legislation, whose main aim is to provide social security, protection, social justice, and regulation. The Indian law categorises workers broadly into Employees, Contractual workers (including contract labour and inter-state migrant workers) and workers employed in the unorganised sector. Although, safeguard measures for workers exist but workers of these online platforms are not governed under any of the including the Contract Labour (Regulation and Abolition) Act 1970, Minimum Wages Act 1948, Employees' Provident Fund and Miscellaneous Provisions Act 1952, Payment of Bonus Act 1965 and Unorganised Workers' Social Security Act 2008. The unique nature of tech-based platforms has made it impractical to be governed under such laws. Thus, with the recommendation of the National Commission on Labour, the Ministry of Labour and Employment introduced the Code of Social Security (2020) that recognises the platform workers as 'gig workers.' The new Labour Code provides definitions of 'gig worker' and 'platform work' but through various judgements, Indian courts, have also provided requirements to be considered when assessing employer-employee relationships. The New Social Security Code of 2020 in this sense distinguishes between employees and gig workers. The Code provides mandatory benefits to employees whereas providing a framework to central and state governments for suitable schemes to benefit gig workers and mandates their registration. The central government is required to establish a social security fund as suggested by the new Code and gig employers are obligated to contribute one or two percent from their annual turnover [Ganguly S., Ramesh A., 2022]. The Code awaits its compliance until state governments make suitable changes in their labour legislations. So, currently, gig and platform workers remain unprotected and unregulated under existing laws. Another section which requires scrutiny is the terms and conditions obli-

[8] Rating Fairness in the Indian Platform Economy: 2020 Fair Work India Scores. Available at: https://fair.work/en/fw/blog/2020-fairwork-india-scores (accessed: 15.12.2020)

gated by the online food aggregator platforms to users and partners. There is arbitrariness in the decision-making in user assistance and refunds.

The rise of platforms has also complicated the legal domain at times moving ahead at a faster pace than law; consequently, the trust in and safety of online platforms will be under scrutiny. The lack of a transparent privacy policy is an example of how the delay in law exposes the population to «platform capitalism".

Conclusion

The convergent and divergent nature of infrastructures and platforms towards each other is the result of constantly evolving innovation in the technology space. The shift towards infrastructure to platforms is in the terms of gap bridged by theirs sharing properties like scale and use. Thus, understanding the rise of platforms is evidence of how infrastructures have transformed into platforms and how platforms have acquired properties of infrastructures. The inquiry into multiple layers of algorithms revealed a clear understanding of the functioning of online food delivery platforms. This also furnished information regarding various contention zones between humans and algorithms, which expanded the horizon of intermediary liability.

Currently, in India the IT Act, Competition Act 2020, and various labour legislations are insufficient or inefficient in protecting the rights of various stakeholders of the platform economy. The online platforms are at present investing in AI technologies, Deep Tech to gain a competitive edge. Thus, a robust and comprehensive legal approach towards current and future technology is required to avoid distrust in technology.

For a country like India, with diverse cultures and languages, platforms need to invest more in the diversification of the workforce and robust business models to make platforms safe for every stakeholder. The government needs to ensure quick and decisive resolutions for technology-based concerns.

References

1. Baldwin C., Woodward C. (2008) The Architecture of Platforms: A Unified View. *Harvard Business School*, no. 9, p. 32. Available at: https://dx.doi.org/10.2139/ssrn.1265155 (accessed: 16.04.2020)

2. Card J. (2017) Financial crises are a 'filtering mechanism' for startups. *The Guardian*. January 24. 2017. Available at: https://www.theguardian.com/small-business-network/2017/jan/24/financial-crises-filtering-mechanism-startups (accessed: 24.01.2017)

3. Chan S., Klareld A.-S. (2022) Platform or infrastructure or both at once? Detangling the two concept's knotty cross-articulations. *Information Research*, no. 27. Available at: https://doi.org/10.47989/colis2205 (accessed: 30.11.2022)

4. Daley J. (2019) Recently Uncovered Thermopolium Reminds us that Romans Loved Fast Food as Much as We Do. *Smithsonian Magazine*. Available at: https://www.smithsonianmag.com/smart-news/romans-loved-fast-food-much-we-do-180971845/ (accessed: 16.04.2020)

5. Davidson N., Infranca J. (2016) The Sharing Economy as an Urban Phenomenon. *Yale Law and Policy Review*, vol. 34*,* no*.* 2, p. 67.

6. Davis G., Shibulal S. (2018) Taming Platform Capitalism to Meet Human Needs. In: S. Rangan (ed.) *Capitalism Beyond Mutuality? Perspectives in Integrating Philosophy and Social Science*. Oxford: University Press, pp. 207–226. Available at: https://doi.org/10.1093/oso/9780198825067.003.0011 (accessed: 11.05.2021)

7. Devendorf L., Goodman E. (2014) The algorithm multiple, the algorithm material: reconstructing creative practice. Available at: https://www.confectious.net/may-15-the-algorithm-multiple-the-algorithm-material-reconstructing-creative-practice-uc-davis/ (accessed: 06.12.2021)

8. Dijck J. van (2013) *The Culture of Connectivity: A Critical History of Social Media*. Oxford: University Press. Available at: https://doi.org/10.1093/acprof:oso/9780199970773.001.0001(accessed: 16.04.2020)

9. Doorn N. (2019) A new institution on the block: On platform urbanism and Airbnb citizenship. *New Media & Society*, vol. 22, no. 10, pp.1808–1826. Available at: https://doi.org/10.1177/1461444819884377 (accessed: 11.05.2021)

10. Doorn N., Mos E., Bosma J. (2021) Actually existing platformization: embedding platforms in urban spaces through partnerships. *South Atlantic Quarterly*, vol. 120, no. 4, pp. 715–731. Available at: https://doi.org/10.1215/00382876-9443280 (accessed: 12.01.2022)

11. Ecker Y., Strüver A. (2022) Towards alternative platform futures in post-pandemic cities? A case study on platformization and changing socio-spatial relations in on-demand food delivery. *Digital Geography*, no. 3. Available at: https://doi.org/10.1016/j.diggeo.2022.100032 (accessed: 04.11.2022)

12. Ganguly S., Ramesh A. (2022) Rules governing India's gig economy. International Bar Association press release. October 7, 2022. Available at: https://www.ibanet.org/rules-governing-india-gig-economy#_edn3 (accessed: 07.12.2022)

13. Ghai D. (2003) Decent work: concept and indicators. *International Labour Review*, vol. 142, no. 2, pp. 113–145.

14. Gillespie T. (2010) The politics of 'platforms'. *New Media and Society*, vol. 12, no. 3, pp. 347–364. Available at: https://doi.org/10.1177/1461444809342738 (accessed: 16.04.2020)

15. Guyer J. (2016) *Legacies, Logics, Logistics: Essays in the Anthropology of the Platform Economy*. Chicago: University Press, 329 p.

16. Iqubbal A. (2021) Food delivery workers in India: emerging entrepreneurs or informal labour? Digital Empowerment Foundation.

17. Jalote P., Natarajan P. (2019) The growth and evolution of India's software industry. *Communications of the ACM*, vol. 62, no.11, pp. 64–69. Available at: doi:10.1145/3347863 (accessed: 16.04.2020)

18. Langlois G., Elmer G. (2013) The research politics of social media platforms. *Culture Machine*, no. 14.

19. Mahadevan K. (2021) Demystifying the Dabbawallahs: India's Lean Food Delivery Operations Explained with Operations Management Practices. *Operations and Supply Chain Management: An International Journal*, vol.14, no. 3, pp. 277–288. Available at: http://doi.org/10.31387/oscm0460302 (accessed: 10.06.2022)

20. Mattelart A. (1996) *The invention of communication*. Minneapolis: University of Minnesota Press, 255 p.

21. Mol A. (2002) The Body Multiple: Ontology in Medical Practice. In: B.H. Smith (ed.). Durham: Duke University Press, 388 p.

22. Mooshammer H., Mörtenböck P. (eds.) (2021) *Platform Urbanism and Its Discontents*. NAi Uitgevers / Publishers Stichting.

23. Mullen A. (2021) Ancient residues, dietary clues. *Nature Food*, vol. 317, no. 2. Available at: https://doi.org/10.1038/s43016-021-00296-8 (accessed: 20.05.2022)

24. Nariman F. (2019) Uber India Systems Pvt. Ltd. vs. Competition Commission of India on 3 September, 2019. Indian Kanoon. Retrieved. Available at: https://indiankanoon.org/doc/152787062/ (accessed: 07.12.2022)

25. Plantin J.-C., Lagoze C., Edwards P. et al. (2016) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media and Society*, vol. 20, no.1, pp. 293-310. Available at: https://doi.org/10.1177/1461444816661553 (accessed: 16.04.2020)

26. Poell T., Dijck J. van, Waal M. (2018) *The Platform Society: Public Values in a Connective World*. Oxford: University Press. Available at: https://doi.org/10.1093/oso/9780190889760.001.0001 (accessed: 16.04.2020)

27. Pujadas R., Curto-Millet D. (2019) From Matchmaking to Boundary Making: Thinking Infrastructures and Decentring Digital Platforms in

the Sharing Economy. In: G. Bowker, P. Miller et al. (eds.) Thinking Infrastructures (pp. 273-286). Tamil Nadu: Emerald Publishing, pp. 273–286. Available at: https://doi.org/10.1108/S0733-558X2019Tamil Nadu0000062017 (accessed: 16.04.2020)

28. Reeves S. (2019) Online food-delivery scrambling more than the restaurant industry. *China Daily. Global Edition*. 20.02.2019. Available at: http://global.chinadaily.com.cn/a/201902/20/WS5c6d7116a3106c-65c34ea6f3.html (accessed: 16.04.2020)

29. Rossi U. (2019) The common-seekers: Capturing and reclaiming value in the platform metropolis. *Environment and Planning C: Politics and Space*, vol.37, no. 8, pp. 1418–1433. Available at: https://doi.org/10.1177/2399654419830975 (accessed:16.04.2020)

30. Scholz T. (2017) *Uberworked and Underpaid: How Workers Are Disrupting the Digital Economy*. New York: Wiley, 310 p.

31. SFLC.in. (2019) *Intermediary Liability 2.0: A Shifting Paradigm*. SFLC.in. Available at: https://sflc.in/sites/default/files/reports/Intermediary_Liability_2_0_-_A_Shifting_Paradigm.pdf (accessed: 20.06.2020)

32. Srnicek N. (2017) *Platform Capitalism*. New York: Wiley, 409 p.

33. Vanolo A. (2014) Smart mentality: The Smart City as Disciplinary Strategy. *Urban Studies*, vol. 51, no. 5, pp. 883-898. Available at: https://doi.org/10.1177/0042098013494427 (accessed: 16.04.2020)

Information about the authors:

N.A. Afifi — PhD Scholar.
R. Sony — PhD., Associate Professor.

The article was submitted to the editorial office 18.11.2022, approved after reviewing 30.11.2022, accepted for publication 30.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Research article
УДК: 342
DOI:10.17323/2713-2749.2022.4.34.51

The Right to Informational Self-Determination: On the Edge of Public and Private

Elvira Vladimirovna Talapina

Russian Presidential Academy of National Economy and Public Administration, 82 Vernadskogo Ave., Moscow 119571, Russia, talapina@mail.ru, https://orcid.org/0000-0003-3395-3126

Abstract

The right to informational self-determination, as the authority of the individual to decide fundamentally for herself, when and within what limits personal data may be disclosed, was formulated by German jurisprudence and has become a model for many States as well as for European Law in general. It is seen as a necessary tool for maintaining a vibrant democracy, on the basis that privacy is an "integral part" of society. The basis for the judicial decision was the Kantian theory of the moral autonomy of the individual. This explains the close connection of judicial reasoning with human rights and their Public Law protection. At the same time, under Anglo-Saxon influence, a "property approach" to personal data which may become the object of transactions is developing. The "property approach" views personal data as a valuable commodity that can be the object of transactions and operations with other people through licenses. In practice, access to personal data has recently been increasingly provided as a counter performance (compensation) to contracts for the provision of digital content and in exchange for personalized services. The study shows there are many interactions of public and private in the legal protection of data (information self-determination as a subjective public right requires the corresponding obligations of the State to be formalized, there is no unambiguous sector qualification of a person's consent to data processing, the insufficiency of the principle of confidentiality by default before the potential for harm is noted). Analysis of the evolution of the data legal protection leads to conclude that the public/private distinction is gradually levelling off. It seems that the problem of the circulation and protection of personal data cannot be solved in a sector framework, but only

comprehensively, without violating the traditional logic of public and private. This means that the right to information self-determination, due to its complex nature, can be regarded as a principle that has an inter-branch nature extends to both the Public Law data protection and the implementation of subjective civil rights in this area.

Keywords

personal data; digitalization; privacy; confidentiality; data treatment; human rights.

For citation: Talapina E.V. (2022) The Right to Informational Self-Determination: On the Edge of Public and Private. *Legal Issues in the Digital Age,* vol. 3, no. 4, pp. 34–51. DOI:10.17323/2713-2749.2022.4.34.51

Acknowledgements: The study was conducted under the research assignment of the Russian Presidential Academy of National Economy and Public Administration.

Introduction

Issues of interpenetration of public and private law arise every minute, but conservative jurisprudence prefers to stay within the branch boundaries. Factors 'diluting' the boundary between public and private law in general, and between branches of public and private law in particular, have been growing in numbers, but the technology factor takes a prominent place: Digitalisation has begun to have a transformative effect on law. Digital technologies, neutral and universal by nature, 'impose' their own logic that levels off the boundary between the public and the private, sometimes causing conflicts with conventional legal routes.

A good theory is of crucial importance for proper and stable development of legislation in general, and for development in the area of information rights of individuals in particular [Arkhipov V.V., 2018: 52-68]. Moreover, this needs to be a well-balanced theory capable of identifying specific features of public law and private law regulators. Today, we need to define very clearly what personal data is, who owns it, how this data is protected and according to what regulations does liability for violations of rights in this area arise. Will this liability be under public law, or private law, or a combination of both of them? In any case, personal data are linked to a physical person, and oftentimes spread by this same individual. Does the 'possession' of personal data impose any obligations on a person? What are the boundaries between public and private interest in using personal data? What are the limits to which a person's right to data extends? These and

other questions are considered in this article, and the author proposes to regard it as an invitation to a discussion.

1. What is the Right to Self-Determination?

Present-day publications note integrative importance of the right to information self-determination in a system of new generation rights that include a range of rules related both to personal freedom and to digitalisation. Historically, information self-determination (Informationelle Selbstbestimmung) was recognised as an independent right in a ruling of the German Federal Constitutional Court[1], which has been extensively commented on in research publications, and not only in Germany.

The dispute centred on the 1983 Federal Census Act, which required the collection of a wide range of data pertaining to the demographic and social structure of Germany. The law established parameters for counting the country's population and required that personal information (name, address, gender, marital status, religious affiliation, occupation, place of work) be provided. The law also required people to answer questions about their sources of income, level of education, mode of travel to work, use of housing, including the way they heat and pay for utilities. Clearly, this information was collected not just for information's sake, but for further use (for planning purposes, environmental protection, etc.), and hence the law allowed the information collected to be passed on to local authorities. These could even compare the information they received with housing registers and adjust them, if necessary.

The provisions of this law became the subject of consideration by the German Federal Constitutional Court (hereinafter–Court). This decision has become a landmark both for the German legal doctrine and for the development of pan-European data protection regulations owing to its obvious and recognised influence on European legal thought.

It is noteworthy that the starting point of the Court's approach was the Kantian theory of the moral autonomy of the individual. This is significant because it explains the close relationship of the Court's reasoning with hu-

[1] Decision of the First Senate of 15 December 1983. — 1 BvR209/83, 1 BvR269/83, 1 BvR362/83, 1 BvR420/83, 1 BvR440/83, 1 BvR484/83 // Selected decisions of the German Federal Constitutional Court. Moscow, 2018, pp. 75-86 (in Russ.)

man rights and their public-law protection. Overall, the Court carried out a profound analysis of personal rights arising deep inside and penetrating various spheres including the information sphere.

As regards personal autonomy, the Court raised the concern that the collection, storage and use of personal information would threaten human freedom. The more you know about a person, the easier it is to control them. On the one hand, in today's information society, control over information means power, which the state seeks to obtain. But on the other hand, control over personal information is the power over one's own destiny, which is necessary to be able to freely open up and develop as a person.

This is why the Court has formulated the right to information self-determination as a kind of counterbalance to the information-gathering activities of the state. Information self-determination is an individual's right to decide when and to what extent their personal data may be disclosed. What is important is that this right was assessed not only retrospectively but also forward-looking: in the Court's view, technological development had already changed the possibilities for gathering information (it is worth reminding that the decision was made in 1983) and will change even more in the future. Indeed, in the past information was entered manually with the help of a punching machine and stored in separate locations, where only specialist staff had access. This made it difficult to obtain a 'portrait' of an individual by linking and combining different data (profiling). Today, almost anyone can enter and retrieve information electronically, which makes it easier to access instantly, and owing to big data technologies, personal information can be to extracted from seemingly unrelated data.

The Court ultimately upheld a large part of the challenged Act, although it did invalidate several provisions, including one that allowed local authorities to compare census data with local housing registers. The basis for such a decision was the possibility of combining these statistics, allowing officials to identify a specific person, thereby violating their rights as an individual.

The Court's reasoning appeared to be highly relevant in the context of separating public and private law. Human dignity, elevated to the top of the value structure, naturally extends to the entire legal system, i.e. both public and private law. Fundamental rights and corresponding duties are an essential part of human dignity [Eberle E., 2012: 224, 227–229].

It is worth noting that the concept of dignity is at the heart of the principle of individualism, which, together with the principle of equality, underlies modern constitutionalism. At the constitutional level, human dignity can be positioned as a principle of law that defines the purposes of or grounds for the adoption of the constitution, a specific human right or a permissible ground for limiting constitutionally recognised rights and freedoms [Vasilyeva T.A., 2020: 98–100].

It is worth mentioning that from a formal legal point of view, the right to information self-determination is not part of the Basic Law (Constitution) of Germany, but it is based on leading principles contained therein. While data protection is not mentioned in the Constitution either, the Court's ruling is based on Article 1.1 of the German Constitution, which states: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority", in combination with Article 2.1 on self-determination "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." Proceeding from these two constitutional provisions, the Court held that the right guarantees a person's ability to determine whether his or her personal data can be disclosed and used. This became one of the first and best known wordings of the right to information self-determination.

The consequences of this milestone decision are significant both for Germany itself, where the principle of information self-determination has since consistently defended by the courts, for other states; e.g., Hungary has followed the German model [Szekely I., Vissy B., 2017: 137], and for European law in general. In Germany, this right is applied to protect quite a broad range of areas. "Designed to ensure a person's authority to make decisions on how others deal with their personal data, the right to information self-determination became a gage for verification whether the computerised suspect identification system, the video surveillance of an art monument located in the town square, the automated collection of vehicle licence plates, the obligations arising from the insurance contract when an insured event is established were in compliance with the Constitution." [Proskuryakova M.I., 2016: 84–98]. And the new European regulation (Regulation No 2016/679 of the European Parliament and of the EU Council 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal

of Directive 95/46/EC (General Regulation on personal data protection)'), using the right to information self-determination, attempts to embed the right to protect personal data into the new digital economy by sharing with the owner the liability for his or her data that the state previously used to regulate. It is the digital challenges that, in our view, allow us to have a closer look at information self-determination, finding in it the potential for adaptation to the modern technology stage.

2. The Right to Self-Determination in the Digital Era

It is hard to argue with the forward-looking, pioneering nature of the court ruling made in 1983, for it did look to the future. That said, this ruling was for obvious reasons based on the data processing technology development level at that time. And, probably, only George Orwell could have foreseen the current situation, where the unprecedented rates of data processing have given rise to a 'surveillance society.' The growing role of data, and transition from data gathering to data transformative use encourage legal discussions in various fields. The topics include the right to digital self-determination, divergent understanding of the ownership of personal data, and the state's protectionist stance on personal information expressed in increased public law protection of personal data.

This broad range coincides in many respects with the two dominant views on the impact of technology on the law as a whole. Supporters of libertarian views believe that the right to data protection may be alienated (sold), while egalitarian scholars lean towards the non-alienation principles, which are necessary to protect individuals from discrimination and stigmatisation, in particular in the socio-economic sphere. Consequently, the first position finds more support in private law and the second in public law.

2.1. Personal Data in Private Law

The personal data concept has its origin in the institution of privacy. The idea to protect privacy through law emerged in the 19th century, at a time when individualism was developing. The starting point for the right to 'informational privacy' is a classic essay by Warren and Brandeis published in 1890 in the Harvard Law Review, which compared the principle of privacy to the right to be left alone, "the right to opacity" [Warren S., Brandeis L.,

1890: 193–220]. The right to opacity protects an individual from being observed, scrutinised or spied on by others in their private sphere.

Following A. Westin's definition [Westin A., 1967: 7], US scholars have traditionally defined the right to privacy, or information confidentiality, as a right of individuals, groups of people, or institutions to independently decide when, how and to what extent information about them is shared with others. This has become the basis for the argument on the existence of an 'intangible property right' that everyone has over their personal data[2], and that people may lawfully 'sell' their personal data on the market thus choosing the best combination of confidentiality without state interference.

The 'property approach' regards data as a valuable commodity that can be the subject matter of transactions effected with other people through a license. In practical terms, access to personal data has recently been increasingly provided as a counter-performance (reimbursement) under contracts for the provision of digital content and in exchange for personalised services.

2.2. Developing a Public Law View

As opposed to the 'information property' theory, proponents of the public law approach point out that information as such does not exist until it is outwardly expressed or disclosed (i.e., information is always to a certain extent constructed.) Consequently, an individual cannot have 'natural', original rights to information or data related to this individual. In this sense, the German court's decision that links information self-determination to the notion of dignity is interpreted as suggesting market inalienability of personal information by default. This view finds support in the attitude towards privacy as not only individual freedom but also an important element of a democracy (based on the assumption that private life is an 'integral part' of society): privacy and data protection are social structure tools for maintaining a free democratic society. Combining these messages culminates in

[2] The theory of 'property right' in respect of privacy has been initiated by supporters of economic analysis of law. In his analysis of confidentiality, Richard Pozner explained that a strong legal protection of privacy may result in negative economic consequences in the labour and loan markets. He believes the beneficiaries of privacy legislation will most likely be people with more arrests or convictions, or with a credit history worse than the average person.

the opinion that information, even if based on personality, is a reflection of social reality and cannot be related linked to a specific individual.

While data gathering aims to profile individuals, controlled persons do not have sufficient means to control such profiling themselves. At the same time, today, the ability to control and influence (in many respects, psychologically) the behaviour of individuals through data collection has increased dramatically. A person's self-determination implies that individuals have the freedom to decide on their actions including the freedom to put their decisions into practice. And if a person cannot with a sufficient degree of certainty forecast what information about them in what areas is known to their social environment, and cannot assess with sufficient accuracy such awareness of the parties the communicate with, then this person is largely limited in their freedom to plan or make decisions without being subjected to any pressure. If, for instance, a person believes that participation in an assembly or other manifestation of civic initiative will be officially recorded and therefore there may be personal risks, this person may refuse to exercise the rights in question. In the Court's logic, this affects not only the individual's chances of free development, but also the common good, since self-determination is an elementary functional condition of a free democratic society based on the capacity of its citizens to act and cooperate. And in general, privacy is more of a social structural imperative of democracy, since as a precondition of democratic discourse is that people feel free to express themselves without fear of being judged, without the possibility that state authorities could interpret their thoughts and behaviour based on the information gathered and processed. It is one of the responsibilities of the state in a democratic society to support and encourage the private and public expression of people's thoughts, preferences, opinions, and behaviour. In other words, privacy regimes and data protection regimes do not exist only to protect the interests of 'rights holders'. In a democratic society they are necessary to keep democracy alive [Rouvroy A., Poullet Y., 2009: 52, 57].

It is worth adding that the 1983 ruling of the Court views individual autonomy not as radical seclusion and independence of the individual in relation to their social environment, but as the autonomy of the individual who is included in society, lives and interacts with others. It turns out that technological development has bridged the gap between private and public law because not only an individual's personal development, but also the public good can be harmed. Incidentally, the idea of joint emergence

and consolidation of private and public autonomy has been taken from Jürgen Habermas:"Valid, legitimate norms of action are only those with which all possible persons who would experience the consequences of accepting those norms would be able to agree as participants in a rational discourse" [Habermas J., 1995: 205]. From a legal perspective this means that individual autonomy, just like a musical or artistic talent, is something that the government would never be able to 'grant' to people through law. "The right to be autonomous' does not have any more sense than 'the right to be happy' " [Rouvroy A., Poullet Y., 2009: 59]. Interestingly, the right to seek happiness does exist in the legal reality (see the US Declaration of Independence).

Moreover, German scholars believe that the decisive argument for understating the right to information self-determination lies in the necessity to distinguish between the legal construct and the theoretical concept at the heart of the underlying law. Therefore, the construct of the right to information self-determination, which states that the processing of personal data by the state constitutes an interference with an individual's right to determine the types and conditions of processing, is not an end in itself, but only a means to protect other basic rights. The theoretical concept here is this instrumental effect of the right to information self-determination. It is becoming increasingly evident from recent court practice that the German Constitutional Court does not interpret the right to information self-determination as strictly individualistic, but rather attaches a strong supra-individualistic dimension to it, which leads to objective demands regarding the processing of information by the state [Marsch N., 2020: 40–41].

Such reasoning forms the basis for a regulatory data protection policy. As an objection to an individualistic interpretation of the right to information self-determination, experts emphasise that data protection legislation protects a whole range of interests, which cannot be regarded as a single legally protected commodity [Albers M., 2014: 213–235].

2.3. Automated decision-making

But online surveillance is not the only threat to individual self-determination. The functioning of automated decision-making systems also calls into question one's self-determination. From a functional point of view, it is essential that automated systems identify and analyse patterns of human behaviour at a level of depth and detail that was previously impossible, and

that they can use these patterns to their advantage. Individual self-determination is threatened by the ever-increasing possibility for somebody else to understand a person's conscious or unconscious behaviour, and to openly or covertly use this knowledge in legal relations to improve their own position — for example by evaluating a person in an exchange of goods, services or information. In fact, this has always been the goal in business and social relations, but digitalisation is giving this process a new quality.

Opportunities for individual self-determination are impaired if the individual never knows what criteria the automated system uses. The literature defines this as insufficient clarity. Automated systems can identify people's characteristics, inclinations, goals and intentions in a previously unknown depth and detail and thus make predictions about their future behaviour. Human cognitive abilities cannot keep up with them, and so the human ability to actually comprehend the specific decision-making processes of automated systems reaches its limit. There is a danger that, if an automated system identifies a certain context and bases its decision on it, humans will no longer understand the automated procedure. And if a person does not know which criteria the automated system uses, their capacity for individual self-determination, which is the basis of the entire human rights construct, is impaired.

In addition, the issue of legal significance of influencing people is of particular importance in legal terms. The main issue here is to determine when such potential for influence is legally significant and when, therefore, should the legal system treat it as a risk to individual self-determination? Basically, it is only the individual who can determine the intensity of the potential for influence. The level of perceived pressure aiming to change a person's behaviour largely depends on individual experience and can hardly be reduced to a particular type. The more personal data automated systems use to influence behaviour, the less transparent they seem, and so the more they influence a person's unconscious and irrational cognitive or intentional processes. The use of randomly appearing criteria can justify the prohibition of automated influences on individual self-determination (the use of criteria that are not predictable and understandable at the individual's current horizon of expectations) [Ernst C., 2020: 60, 62].

It should also be borne in mind that many persons tend to coordinate their behaviour with the behaviour of others. For an individual the approval of the masses can make a certain decision credible, but it can also create

an obstacle that would prevent deviating from that decision. Depending on the design of the decision-making system, there may be a concentration of behavioural patterns and a convergence of individuals. The number of options available to an individual may tend to reduce and focus on core behaviours and decisions. Then the realisation of individuality may require more efforts and expenses, and may even lead to social divisions.

These concerns are often cited as an argument for strengthening the right to information self-determination, both in public and private relations.

3. Mixed Interpenetration of the Public and the Private in Data Protection

3.1. Information self-determination as a public right

While the above views on the nature of personal data might seem diametrically opposed, this should not give the reader the wrong idea. In actual fact, there is a lot of overlap in both the approach and the regulation of these issues. To some extent, the theory of subjective public rights emerged at the crossroads of public and civil law. Can the right for information self-determination be considered a subjective public right?

As I.A. Pokrovsky wrote in 1917, after the collapse of the natural law doctrine, the positivist jurisprudence of the first half of the 19th century denied the grounds for constructing a person's subjective rights: The law protects life, physical integrity or honour of people, but there are no civil rights to life, freedom, etc. An individual's civil right only arises at the time a certain legal prohibition is breached and pertains only to the compensation of the losses incurred [Pokrovsky I.A., 1998: 122]. And while an individual's interests (right to name, image, honour and dignity) penetrated civil law soon enough, the logic of protecting them originates from the logic of loss.

At the same time, in the same work of Pokrovsky we find that "civil law was originally and by its very nature the right of the individual human being, the sphere of his freedom and self-determination." [Pokrovsky I.A., 1998: 309]. If we stick to the word 'self-determination', can we argue that information self-determination is one of these individual rights protected by civil law?

This question needs to be approached pragmatically, and the interests of the individuals themselves need to be taken into account. It is clear that

quick and widespread technology development can result in the suppression of individuality. Qualifying information self-determination as a public right may ultimately prove more advantageous for people because, in addition to the subjective aspect of the rights that citizens can exercise, the objective aspect of the rights that they can claim from the government and its bodies are also assumed. This is the way the fundamental rights are in the constitution.

But even this may not be enough. In some jurisdictions, fundamental rights do not extend to the private sector, but in most cases constitutional provisions are binding on the private sector, too (which is to some extent a declaration, since private actors need substantive laws). In addition, it would be a good idea to equip the right to information self-determination with both criminal liability measures and civil redress mechanisms, i.e. to provide comprehensive protection.

3.2. Consent to personal data processing

The institution of consent to personal data processing has a significant role to play. Actions that would otherwise be illegal become legal through consent. It would be appropriate here to consider this problem from a geographic perspective (Europe — USA) and from a public/private perspective.

The EU has a some sort of paternalistic approach to data processing: EU law requires a much stricter and more explicit form of consent than US law. Moreover, EU law restricts the gathering, use and disclosure of data (a legal basis for personal data processing is required), whereas in the US, data can generally be processed unless the law specifically prohibits it.

This does not necessarily mean that more explicit EU consent requirements will necessarily lead to people undertaking a more meaningful cost-benefit analysis of the collection and use of their data. But it takes more efforts and is more expensive to obtain consent under EU law. In today's world, the formal approach taken in EU regulations is rather a drawback because restrictions are often stipulated without any link to harm. As a result, regulation can prevent processing that does no harm and may even be beneficial. US law, on the contrary, usually permits data processing if it does not cause problems. [Solove D., 2013: 1900]. This situation has encouraged many researchers to take a closer look at the US approach owing to its flexibility and practicality.

Qualification of consent differs in public and private law. The civil law literature suggests that, by analogy with consent to the use of an image, consent to the processing of personal data should be treated as a transaction, and that as a result withdrawal of consent, the person who had the right to process such data could impose a civil penalty [Savelyev A.I., 2021: 104].

Proceeding from a serious attitude to the fundamental principles of data protection and rejecting the 'information market' approach, public law scholars criticise the tendency to view individual consent as a sufficient criterion for the legitimacy of any kind of data processing [Rouvroy A., Poullet Y., 2009: 74]. They give an important role here to human rights, which ensure the autonomy of individuals in a free and democratic society. The 'classic' privacy and data protection regimes should be seen together as forming an evolving bundle of legal protection tools for the fundamental individual and social structural value of individuals' autonomous capabilities. At the same time, scholars propose to strengthen the right to information and to grant new rights to consumers, including class actions, which again brings the issue to the intersection of the public and the private.

To outline the view of the Russian doctrine and practice on this issue, we would like to note Ruling of the Russian Federation Constitutional Court of 26 October 2017 No. 25-P "On the Case of Checking the Constitutionality of Article 2 Paragraph 5 of the Federal Law "On Information, Information Technologies and Information Protection" in connection with complaint of citizen A.I. Sushkov." This ruling attempts to evaluate a user agreement that assumes the existence of differentiated rules regarding access to user data. However, this attempt cannot be considered sufficient or successful.

3.3. Privacy by default or minimum harm?

The basic principle of data processing under the European Regulation (and, consequently, under Russian law, and even, to a certain extent, Chinese law[3], both of which follow European law in these matters), namely the principle of 'privacy by design', makes it obligatory to process only the personal data that is necessary for each specific purpose of processing. However, data minimisation has been getting increasingly problematic and, given

[3] See: Personal Information Protection Law of the People's Republic of China // Available at: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ (accessed: 23.03.2022)

the growing proactivity of actors alongside with the collection of data in the process of total surveillance, hardly feasible at all. In view of this, the literature suggests that 'privacy by design' be transformed to 'minimum harm by design.' [Orrù E., 2017: 107–137]. The difference between MHbD and PbD is that, firstly, it recognises that possible harm from surveillance goes beyond only violating privacy and attempting to provide guidance on how to remedy such violations; secondly, the burden of proof shifts to the surveillance parties. In essence, the proposal seeks to recognise the inevitable harm to privacy in the modern digital society and to respond to breaches in the general logic of civil law, with procedural preferences for holders of personal data.

The above issues provide a clear illustration of a real confusion between public and private law approaches to data protection, along with the state of incompleteness of legal protection of data.

4. Data protection as a concept indifferent to the division of law into public and private

Based on an analysis of the evolution of data protection, scholars conclude that the public/private division has been gradually levelling off. E.g., in German law, the evolution of legal protection of personal data was mainly based on a hierarchical concept aimed at protecting the individual from the state. But following the establishment of personal data protection legislation, the traditional distinction between public and private law was challenged. This resulted in a unitary approach to regulation, regardless whether the data controller is a government agency or a private company. This is also true with respect to the European legislation on the protection of personal data. The new Regulation requires private data processors to balance their own interests with those of the individual whose data is processed. The Western literature regards this as "a most difficult and almost schizophrenic task", especially for young companies and lawyers.

The US privacy law, on the other hand, largely attempts to increase individual freedom, including the commercialisation of personal facts (right of publicity) [Sattler A., 2018: 30, 36]. It also contributes little to division between the public and the private, which is not close to the Anglo-Saxon legal system in any case.

Thus, we have to note the erosion of the boundary between the public and private spheres. In these circumstances, the idea of data ownership is

evolving, and this process is encouraged from both sides. Firstly, private law has been based on the principle of autonomy from the outset, thereby emphasising the freedom to act according to one's will, so it is logical to give one the right to dispose of one's data. Secondly, it pushes the development of technology. There is no need for in-depth research to prove that an individual's consent to data processing, in the form of a check in the box on a website, bears little resemblance to informed and conscious consent as required by the European Regulation. Such consent has even been compared to a deal between an explorer and a native on a far-away shore in the sixteenth century, with the difference that access to personal data is exchanged for sparkling glass beads [Sattler A., 2018: 40].

Certainly, the idea of personal data ownership seems attractive against this background. Since data has already become 'the new oil' and the process of data circulation is inevitable, it should be channelled in a civilised and regulated way. This has always been the legal logic.

However, a dive into the subject reveals a range of problems related to the fact that personal data, for obvious reasons, is not a subject matter of civil law and therefore the traditional civil law institutions simply do not focus on it. Let us recall that property in civil law can be linked to things (property right) and to intangible assets (intellectual property right). If a property right to personal data arises, it needs to be clearly defined. This is where the views differ significantly — should it be regarded as intangible good, as a subject matter of intellectual property rights, or as other property?

A.I. Savelyev characterises the evolution of the civil law definition of personal data as a gradual movement from personal non-property to property of a special kind, which falls under the category of other property under Article 128 of the Russian Civil Code. Civil law doctrine also raises the question of treating personal data as a counter-performance [Savelyev A.I., 2021: 129]. Of further note is the proposal to apply the relatively well-established regulations on intellectual property to Big Data [Sergeyev A.P., Tereshchenko T.A., 2018: 121]. This suggestion could well be applied to personal data.

International literature has also made references to copyright in this area and suggests some modification. A true empowerment of individuals whose data is processed can be made easier to attain by introducing a dual-

istic right. Such a right — in many ways similar to early copyright — can be a property right that allows the individuals in question to benefit economically from the use of their data. Here, suggestions are made to eliminate the inconsistencies between contract law, copyright and data protection law. At the same time, since personal information is diverse and highly context-sensitive, the right to personal data should (again by analogy with moral rights in early copyright law) be coordinated with due respect for human rights [Sattler A., 2018: 48].

It seems that the problem of the processing and protection of personal data cannot be solved within a particular area, but only in a comprehensive way, without violating the traditional logic of public and private. Let us try to summarise the results.

In Lieu of a Conclusion

The right to information self-determination is at an intersection, of sorts, between public and private law, the challenges of new technologies, and individual and public interests. It may well be that its successful resolution will serve as a model for building future legal regulation in a digitalised environment. We believe that the following needs to be taken into account.

Two approaches to the right to information self-determination are seen clearly. The original US approach to privacy self-management based on the notice and choice mechanism has been criticised in European doctrine as facilitating commercial exploitation of personal data and endangering user privacy, identity and dignity [Vivarelli A., 2020: 305]. In turn, Americans call the European approach excessively paternalistic [Solove D., 2013]. But despite their seeming polarity, these approaches can be combined, as long as we do not consider data protection to be solely a matter of private or public law.

The 'origin' of data protection from privacy protection has played a two-fold role. On the one hand, the fact that private life was initially reflected in civil codes has placed its protection at the level of a civil right protected individually in the event of a violation. On the other hand, the increasing interference of the state in this area has created the basis for its constitutional recognition, following which data protection took on a life of its own. The rights to privacy and personal data, recognised as human rights, strengthen the public-law component.

No matter how it is defended, the right to information self-determination is not absolute and may be restricted in the public interest. From the personal data owner's point of view, this also outlines the limits of their own responsibility because it cannot be left to the individual to determine the fate of the data. The state and its institutions have an important part to play, too.

It was long noted above different attitudes to information in public and private law: openness and privacy, respectively. Public law adds general guarantees by working through the institution of human rights, which acts as a guarantor of human-centred perspective in relation to the use of technology. At the same time, the growing tendency to apply civil law constructs in public law has an explanation: their resilience and stability have for centuries been successfully combined with flexibility and freedom, (relatively) independent of political change. What is also appealing about the civil law approach is that it is pragmatic.

The general context of modern governance, the focus on a social state and involvement of the private sector to public tasks, leads many jurisdictions to believe that a whole host of issues, including data protection, are cross-sectoral and do not recognise the public/private distinction. Therefore the right to information self-determination can become a cross-sector principle that extends to both public data protection and the exercise of subjective civil rights. The comprehensive nature of this data protection principle involves building both public and civil law protection mechanisms combined with a subtle approach to the balance between their basic components.

References

1. Albers M. (2014) Realizing the complexity of data protection. In: Gutwirth S., Leenes R. et al. (eds.). Reloading data protection: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, pp. 213–235.

2. Arkhipov V.V. (2018) Personal Data as nonmaterial values (or there is nothing more practical than a good theory). *Zakon*=Statute, no. 2, pp. 52–68 (in Russ.)

3. Eberle E. (2012) Observations on the development of human dignity and personality in German constitutional law: an overview. *Liverpool Law Review*, no. 3, pp. 201–233.

4. Ernst C. (2020) Artificial intelligence and autonomy: self-determination in the age of automated systems. In: T. Wischmeyer, T. Rademacher (eds.) Regulating artificial intelligence. Cham: Springer, pp. 53–74.

5. Habermas Yu. (1995) Democracy. Reason. Moral. Moscow: Academia, 245 p. (in Russ.)

6. Marsch N. (2020) Artificial intelligence and the fundamental right to data protection: opening door for technological innovation and innovative protection. In: T. Wischmeyer, T. Rademacher (eds.). Regulating artificial intelligence, pp. 33–52.

7. Orrù E. (2017) Minimum Harm by Design: Reworking privacy by design to mitigate the risks of surveillance. In: Leenes R. et al. (eds.) Data protection and privacy: (in)visibilities and infrastructures. Cham: Springer, pp. 107–137.

8. Pokrovskiy I.A. (1998) Main issues of civil law. Moscow: Statut, 353 p. (in Russ.)

9. Rouvro A., Poullet Y. (2009) The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth S. et al. (eds.) Reinventing data protection. Dordrecht: Springer, pp. 45–76.

10. Sattler A. (2018) From personality to property? Revisiting the fundamentals of the protection of personal data. In: Bakhoum M. et al. (eds.) Personal data in competition, consumer protection and intellectual property law: towards a holistic approach? Heidelberg: Springer, pp. 27–54.

11. Savelyev A.I. (2021) Civil law aspects of commercialization of personal data. *Vestnik grazhdanskogo prava*= Civil Law Herald, no. 4, pp. 104–129 (in Russ.)

12. Sergeev A.P., Tereshchenko T.A. (2018) Big data: in search of a place in the civil law system. *Zakon*=Statute, no. 11, pp. 106–123 (in Russ.)

13. Solove D. (2013) Privacy self-management and the consent dilemma. *Harvard Law Review*, vol. 126, pp. 1880–1903.

14. Szekely I., Vissy B. (2017) Exercising access rights in Hungary. In: C. Norris et al. (eds.) The unaccountable state of surveillance. Exercising access rights in Europe. Cham: Springer, pp. 135–180.

15. Umnova-Konyukhova I.A., Alferova E.V., Aleshkova I.A. (2021) Digital development and human rights. Moscow: INION, 174 p. (in Russ.)

16. Vivarelli A. (2020) The crisis of the right to informational self-determination. *The Italian Law Journal*, vol. 6, no.1, pp. 301–319.

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

18.Westin A. (1967) *Privacy and freedom.* New York: Atheneum, 487 p.

Information about the author:

E.V. Talapina — Doctor of Sciences (Law), Doctor of Law (France), Chief Researcher.

The article was submitted to the editorial office 05.09.2022; approved after reviewing 30.10.2022; accepted for publication 09.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Research article
УДК: 342
DOI:10.17323/2713-2749.2022.4.52.66

State Regulation and Deregulation: A Case of the Communication Industry

Ludmila Konstantinovna Tereschenko

Institute of Legislation and Comparative Law under the Government of the Russian Federation, 34 Bolshaya Cheremushkinskaya Str., Moscow 117218, Russian Federation, adm2@izak.ru

Abstract

The paper is focused at the correlation of state regulation and deregulation in the communication industry. The regulation of major sectors such as the communication industry should be up to the challenges of today. In the current context of building a new digital economy and reducing administrative barriers, a special importance is attached to how state regulation and deregulation correlate in the communication industry. The paper provides an analysis of regulation in the industry to identify the sectors may be excluded from state regulation or may benefit from self-regulation or deregulation. It purports to identify (based on analytical findings) the existing trends in the way the public authorities use regulation and deregulation in the communication industry. With this purpose, the author studied possible vectors of deregulation and reviewed the sectors that were more deeply deregulated and those that could benefit from both regulation and deregulation. With the communication industry constantly progressing and the technologies improved, new social relationships not covered by regulation and not subject to deregulation emerge. Thus, the paper also deals with the problem of legal gaps. The methodology involved is a combination of academic research methods, with both general and special (including formal legal and technical) methods used. The research findings are summarized in the form of short conclusions.

Keywords

communication industry, telecommunications, state regulation, self-regulation, deregulation, gap, telecom operator.

For citation: Tereschenko L.K. (2022) State Regulation and Deregulation: A Case of the Communication Industry. *Legal Issues in the Digital Age*, vol. 3, no. 4, pp. 52–66. DOI:10.17323/2713-2749.2022.4.52.66

Introduction

State regulation and deregulation demonstrate a variable balance in specific sectors at different development stages of economic relationships for a number of reasons. Regulation may be abandoned (with no statutory regulation in place) for a number of factors. There may be social relationships which:

the authorities do not consider necessary to regulate;
cannot be efficiently regulated by law;
cannot be regulated by law at all.

The dynamic boundaries between these groups will change as specific social relationships develop. The regulatory efficiency/inefficiency and absence of social need in strict regulation is one of the main criteria behind the choice of the model to shape social relationships. The view of E.P. Gubin is remarkable in this regard: "the development of law assumes not only the adoption of new regulations but also "deregulation" of economic relationships" [Gubin E.P., 2022: 36–46].

The modern society has a variety of social regulators, with law being just one of them. As observed in literature, the ever shrinking economic share of the state as a result of privatization, liberalization and deregulation is characteristic of the current stage of economic development in a majority of developed economies [Markvart E., Kurbanov B., 2018: 61-78]. However, deregulation does not mean zero regulation where law as a regulator gives place to other regulators of social relationships.

1. Deregulation and self-regulation

Self-regulation is often believed to be a variety of deregulation.

The main piece of legislation governing the legal status of self-regulated organizations (SRO) in Russia is Federal Law No. 315-FZ "On Self-Regulated Organizations" dated 1 December 2007 which identifies the main requirements to SRO as the legal basis for the emergence of such entities.

The definition of self-regulation given in Article 2 of this Law is instructive for the purpose of this paper. Self-regulation is understood as an

independent and self-motivated activity pursued by agents of a specific business or trade to develop and establish the standards and rules of the given business or trade and to exercise control of compliance with these standards and rules. While regulation is obviously there, legal provisions will give place to the standards and rules established by the business/trade agents themselves. Moreover, these standards and rules are binding on all members of a self-regulated organization. From this perspective, it would be wrong to speak of zero regulation or deregulation as such: regulation is passed to a different level, with membership in a self-regulated organization conditioned by compliance with the established rules and standards. Control is also there: however it is exercised not by the government but rather by the self-regulated organization and with higher efficiency in a number of cases than the public authorities would achieve.

According to Yu. A. Tikhomirov, self-regulation is a system of governing the affairs of society by way of self-organization and independence [Tikhomirov Yu.A., 1994: 193–213]. However it should be said that self-organization and independence are underpinned by a permitting regime established by the state out of the public interest. Where market players cannot reconcile their interests in a certain area, the state should deal with the issue by identifying the most optimal ways and methods of impact.

There is no self-regulation of the communication industry in the full sense though telecom operators attempt to address certain issues by concerted efforts. As to deregulation, this goal was set long time ago but failed to be widely pursued.

Deregulation is believed to be one of the principal ways for overcoming administrative barriers. "It does not mean that regulation is abandoned as such but that it assumes only minimal restrictions required to protect the state and society, regional communities and trades, individuals and legal entities" [Khabrieva T.Ya., Marcou J., 2011]. Moreover, deregulation results in more flexibility and adaptivity to the renewed social relationships.

Meanwhile, it follows from practice that deregulation will often involve the interventions of a different nature and focus. For instance, under the 2006-2008 Medium-Term Socioeconomic Development Programme approved by Government Resolution No. 38-r of 19 January 2006[1], it was decided to take the following steps for deregulation of the communication industry:

[1] Collected Laws of Russia. 2006. No. 5, p. 589.

direct regulation of tariffs for communication services to give place to the control of fair pricing in compliance with legal provisions;

cross subsidization to be phased out;

market mechanisms to be developed and transparency of radio spectrum allocation improved;

arrangements for allocation of numbering resources to be improved by way of transition from lump sum to regular payments to be differentiated depending on the extent the resource is used;

control and supervision procedures with regard to economic agents in the communication industry to be improved and made less cumbersome.

Only the transition from direct regulation of prices and tariffs to the control of fair pricing in the sector could be regarded as deregulation. The abandonment of direct regulation of prices and tariffs is one of the main vectors of deregulation. Its pursuit demonstrates efficiency in competitive market segments. Therefore, direct regulation of prices and tariffs in the communication industry is feasible as long as there is competition.

In this regard, it is instructive to refer to the Federal Antimonopoly Service position outlined in its decision of 31 March 2017 in connection with case No. 1-10-141/00-03-16: "Deregulation is only needed where the conditions are created for true rather than pseudo market competition. For this reason, this issue should be addressed selectively and on a case-by-case basis"[2].

As part of this approach, the FAS of Russia has approved the price ceilings for communication services, within which telecom operators are free to set tariffs. Here are some examples. The FAS order of 19 February 2019 (No. 192/19[3]) approved the maximum tariffs for public communication services to be provided by PAO Tattelecom in Tatarstan as well as the maximum tariffs for local telephony services, intrazone connections between subscribers/users of fixed telephone lines for transmission of voice and facsimile messages and data, and for inland telegram services to be provided by PAO Tattelecom in the said territory.

Similar decisions were made in respect of PAO MGTS in Moscow: order No. 1843/18 of 25 December 2018[4] approved the maximum tariffs for

[2] SPS Consultant Plus.

[3] Available at: http://www.pravo.gov.ru (accessed: 31.01.2019)

[4] Available at: http://www.pravo.gov.ru (accessed: 29.01.2019)

local telephony services to be provided by PAO MGTS in the territory of Moscow, and for intrazone connections between subscribers/users of fixed telephone lines for transmission of voice and facsimile messages and data. At the same time, the FAS approved order No. 1842/18 of 25 December 2018[5] applicable to tariffs for local, intrazone telephony connections and inland telegram services to be provided by PAO Bashinformsvyaz in Bashkortostan.

The maximum tariffs also cover the digital signals delivery services from the nationwide mandatory public TV and radio channels to radio electronic facilities for broadcasting[6].

The elimination of cross subsidizing is designed to improve financing in the industry but does not in any way affect the deregulation process. The development of market mechanisms and more transparent allocation of radio spectrum likewise bear only partially relation to deregulation since Article 22 of the Federal Law "On Communications" gives the Government an exclusive right to regulate the use of the radio spectrum. Moreover, while market mechanisms are allowed to be used at different stages of the radio spectrum allocation and use, they are subject to legal provisions and do not exclude state regulation.

The mechanisms for allocation (including improvement) of the numbering resources do not provide for deregulation either. Moreover, these resources, being scarce, make a case for state regulation and control, something which does not rule out the possibility of engaging market mechanisms as part of regulation.

Making the procedures for control and supervision of economic agents more efficient and less cumbersome is a general trend and a policy pursued by the state that does not exclude regulation.

It is worth noting that there is no universally acknowledged concept of "deregulation". Thus, the authors of the book "Statutory Regulation of Economic Relationships" [Gubin E.P., Karelina S.A., 2018] believe that "deregulation" should not imply the processes of removing the state from the

[5] Available at: http://www.pravo.gov.ru (accessed: 06.12.2018)

[6] See FAS Order No. 1540/18 of 12 November 2018 "On Approving the Maximum Tariffs for the FGUP Russian TV and Radio Broadcasting Network Services to Deliver Digital Signals of Nationwide Mandatory Public TV and Radio Channels to Radio Electronic Facilities for Broadcasting" // SPS Consultant Plus.

market: deregulation is also an economic regulatory tool for the government which can be associated with the methods of direct impact.

One has to agree with A.V. Dyomin [Dyomin A.V., 2017] that "deregulation normally means the abandonment of imperative methods in favour of alternative expansion of independence of private individuals at the expense of the powers of regulating agencies". We believe that deregulation can be regarded broadly as the legislative changes focused at more empowerment and independence of economic agents and at the *relaxation* of regulation, while narrowly — as the substitution of regulation with other social regulators, with specific relationships exempt from it.

Deregulation is a general trend in a majority of countries since it is regarded as one of the main policies supporting the innovative economy. However, it is far from being considered a totally positive phenomenon. As a number of researchers point out, deregulation has negative implications in the form of higher uncertainty within society in the absence of transparent state leverage [Baumann S., 2005: 27, 53–54]; [Nozdrachev A.F. et al., 2015]; [Khabrieva T. Ya., Marcou J., 2011].

In support of this idea, other authors observe with regard to the outcomes of globalization that "the leading capitalist countries, while imposing on the world the maximum economic openness, decentralization and deregulation, are building up a centralized, sovereign and regulated market mechanism whose vested interests are ensured and protected by a powerful state machinery, credit facilities, information and military infrastructure" [Krasinsky V.V., 2017].

There is a yet tougher line on deregulation as it is believed that deregulation does not provide opportunities for the development of new technologies and, most importantly, will reduce the room for the government's control over the national economic development in peripheral countries. As observed by A.Yu. Novoseltsev, "the countries that embark on economic deregulation lose the national jurisdiction even over national, not to mention international, companies" [Novoseltsev A.Yu., 2022: 10–13].

In many cases, globalization has deregulated or made labor markets more flexible, only to mean in practical terms the amendment or abolition of labor laws which prevented layoffs, wage reductions, changes to social security systems", etc. [Kovalev A.A., 2013: 115–116].

Deregulation is often used in the fight for foreign investments to remove as many restrictions as possible, primarily with regard to labor, and to ensure cheap workforce for investors into the sector. However, with automation as a new trend, cheap workforce will cease to be the factor capable of attracting and encouraging investments.

Anyway, the deregulation policies that provide for fewer restrictions should be at least as justified and well-founded as regulatory tightening.

Since less regulation assumes more competition, it is instructive to look into the provisions of Presidential Decree No. 618 of 21 December 2017 "On the State Policy Guidelines for the Promotion of Competition"[7] that has approved the 2018-2020 National Plan for the Promotion of Competition. The policies for communications include, for example, the support for innovative infrastructures on the principles of non-discriminatory requirements to market players irrespective of the technologies they use to provide their services; a choice between at least 3 providers of signal transmission services in minimum 80 percent of cities populated by more than 20 thousand people; the elimination of unfair tariff differentials for mobile services provided to travelers (nationwide roaming)[8]. The said policies primarily purport to do away with monopolies in the market for communication services and to create a competitive environment through legal means. This document does not obviously deal with deregulation of the communication industry.

Meanwhile, it is worth noting that a rapid progress of infrastructure sectors, primarily that of telecommunications, and the use of new technologies help to do away with monopolies in the market for communication services, in particular, by reducing the costs involved in the installation of fiber optic lines (replaced with satellite connectivity in a number of countries) while Russia with its vast territory still has to install more communication lines. De-monopolization of the industry as a result of technological change will relax state regulation as well.

The Digital Economy of the Russian Federation Programme[9] adopted in July of 2017 has multiple references to a need to remove barriers including

[7] Collected Laws of Russia. 2017. No. 52 (Part I), p. 8111.

[8] See more below.

[9] Approved by Federal Government Resolution No. 1632-r of 28 July 2017, voided since 11 February 2019. See: Collected Laws of Russia. 2017. No. 32, p. 5138.

in the sector of telecommunications, a task that was interpreted broadly but did not involve deregulation. The subsequent National Programme of the Digital Economy for the Russian Federation[10] identified normative regulation of the digital environment as one of the main policies aimed, as follows from the text, at drafting and adopting a number of regulations to remove priority barriers in the way of digital economic development, in particular, in such sectors as telecommunications.

There is an ongoing process of regulating overarching legal issues related to the identification of the parties to legal relationships, e-document flow, collection, storage and processing of data including personal information. As follows from the Programme, the set of interventions will spill over, in particular, to other domains and branches of law as the priority sectoral objectives and general systemic issues of establishing a single digital environment of confidence are met.

Evidently, this document likewise does not explicitly envisage deregulation of relationships including in the communication industry — it deals, on the contrary, with regulation. Meanwhile, it is worth noting that deregulation of specific areas of social relationships could be willed by the state in the form of legal provisions, i.e. can result from regulation.

Less regulation effectively implies a reduction of natural monopoly stakes in the given sector. Federal Law No. 147-FZ "On Natural Monopolies" of 17 August 1995[11] contains a list of natural monopoly spheres which include, in particular, the public telecommunication and postal services. With the technological change and emergence of new technologies, a monopoly can cease to be natural as observed in the communication industry where alternative solutions, new communication types and services come to be used in the public interest. The extent of state regulation in this sector will change accordingly. Moreover, whether there is a public interest is principally important.

Natural monopolies are mainly regulated through tariffs: the communication industry is no exception. Deregulation of this kind will improve the flexibility and resilience of the Russian economy and promote fair market

[10] Approved by the Presidium of the Council for Strategic Development and National Projects under the President of Russia, Protocol No. 16 of 24 December 2018 // SPS Consultant Plus.

[11] Collected Laws of Russia. 1995. No. 34, p. 3426.

(competitive) pricing of communication services. Presidential Decree No. 618 of 21 December 2017 "On the State Policy Guidelines for the Promotion of Competition" that approved the 2018-2020 National Plan for the Promotion of Competition provides, in particular, for the national legislation to be amended to remove unfair tariff differentials for mobile telephony services for users traveling across Russia within the coverage of one and the same telecom operator.

This objective is already being implemented: under Federal Law No. 527-FZ of 27 December 2018 "On Amending Articles 46 and 54 of the Federal Law "On Communication" effective since 01 June 2019, mobile telephony operators should guarantee equal service conditions to each subscriber in their networks irrespective of the region he or she is located in. Also, Telecom operators cannot charge fees for incoming calls from other regions of Russia.

It is worth noting an obvious trend of the changing structure and volumes of the telecommunication market. As the Government reported back in 2011, with the growing market for web-based services, the traditional communication services in the VOIP segment were being replaced with web-based mobile technologies. In the segment of local and intrazone telephony, mobile telephony services were the main substitute while IP telephony was used likewise in the segment of international and intercity telephone services[12]. The aforementioned provisions will make this trend even stronger. As a result, a considerably lower need in specific communication services may relax regulation.

While the newly adopted laws undoubtedly serve to protect communication service users, they cannot be regarded as dealing with deregulation of this industry. On the contrary, it was the Government's will to change the situation favourable to telecom operators through amendments to the effective law that allowed to ensure a level field for provision of services. Market mechanisms failed in this case as all telecom operators strived to make more profits. The best international practices were equally ignored. Such situation could only be changed by the state through a focused regulatory intervention.

[12] See Federal Government Ordinance No. 1540-r of 06 September 2011 "On Approving the Socioeconomic Development Strategy of the Central Federal District for the Period until 2020". Collected Laws of Russia. 2011. No. 39, p. 5489.

In a number of cases, the duty of changing the current regulatory regime can be based on Constitutional Court rulings to acknowledge certain provisions of law contrary to the Constitution. This is a case for exclusive state regulation which is essentially a duty of the legislator.

An obvious example is Constitutional Court Ruling No. 2-P of 28 February 2006[13] to recognize paragraphs 2 and 3, Articles 59 and 60 of the Federal Law "On Communication" as contrary to the Constitution of Russia. These provisions deal with the duty of operators of public communication networks to make deductions to the universal service fund for compensation of losses caused to universal service operators in the course of service provision.

While the amount of deductions is the same, their nature is totally different: previously non-tax, they become state-imposed tax payments subject to the general provisions of the Tax Code complemented with those governing calculation rules and due dates, with tax collection enforced by the state. This problem was likewise solved exclusively by state regulation: while self-regulation was possible in theory, it would require a party (self-regulated entity) to regulate the social relationships in question and make sure all members comply with the established obligations. The required conditions are obviously not there yet.

State regulation is tightening in certain areas of telecommunications largely due to the need to provide public authorities with reliable information including on subscribers. Thus, Federal Law No. 533-FZ of 30 December 2020 "On Amending the Federal Law "On Communication" has come to include Article 44.2 initially entitled "The information system for monitoring compliance of telecom operators with their duty to check the validity of subscriber details and those of the users of subscriber services (to be provided by legal entities or private entrepreneurs)", now entitled "Monitoring of Telecom operators' compliance with their duty to check the validity of subscriber details and those of the users of subscriber services (to be provided by legal entities or private entrepreneurs) including services provided by the persons acting on behalf of telecom operators".

For the purpose of monitoring telecom operators' compliance with their duty to check the validity of subscriber details and those of the users of subscriber services (to be provided by legal entities or private entrepreneurs),

[13] Ibid. 2006, No. 11, p. 1230.

this Article requires to put in place a data system integrated into the universal identification and authentication system, the database of migrated subscriber numbers, and other information systems.

State regulation serves to a large extent to facilitate rather than reduce the established procedures by making them digital and remotely executable. Thus, the communication industry was among the first to adopt a register-based model for provision of public services.

As a general trend in development of e-services, they are available without a need to visit public agencies. Thus is achieved, in particular, through the use of the register-based model which does not require to issue a paper document as a result of the service provision: it is the entry to the corresponding register that has a legal value.

Federal Law No. 478-FZ of 27 January 2019 "On Amending Specific Regulations of the Russian Federation Regarding the Register-Based Model for Provision of Public Licensing Services for Specific Activities" has taken effect on 01 January 2021 practically at the same time as Federal Law No. 509-FZ of 30 December 2020 "On Amending Specific Regulations of the Russian Federation" also aimed at introducing the register-based model for provision of public services. The said regulations extend this model to the licensing sector, one of the vital for businesses, by replacing paper licenses with electronic entries [Kucherov I.I., Sinitsyn S.A., 2022].

In our view, there is another noteworthy aspect. Zero regulation of specific social relationships is not tantamount to deregulation. This could signal a legal gap to be eliminated in view of certain circumstances and enforcement problems which are there. These relationships could be subject to regulators of the non-legal nature. From this viewpoint, it is instructive to invoke L.A. Morozova's position in respect of imaginary legal gaps she believes to be intentional silence of the legislator, that is, where a question is deliberately left to the enforcer's discretion or where social relationships are purposefully removed from the regulatory scope [Morozova L.A., 2002]. This approach to distinguish between the imaginary and real gaps has to be made clear. Real problems can emerge either simultaneously with the adoption of a specific law or some time later. This might happen, for example, as a result of the technological change which directly affects the emerging relationships. While new technologies bring about new relationships to be regulated, this may result in legal gaps.

In distinguishing between deregulation and a legal gap, it is useful to refer to the definition given by V.S. Nerseyants whereby a legal gap it is the absence of a provision which would be needed, under the logic of the effective law and by the nature of the social relationships in question, to regulate a situation (relationship) covered by the current regulation [Nerseyants V.S., 2001]. A gap is unlikely to be intentional and purposeful, despite a need in regulation, otherwise it would amount to deregulation which allows for the absence of specific provisions.

There is a view in the doctrine that delegation of public authorities can also amount to deregulation [Romanovskaya O.N., 2017: 143–154]. However, the author justly observes, deregulation will involve the abandonment of state regulation, with private entities likely to fill the emerging void in governance. We believe that, as regards delegation, the state does not step back; it will exercise control over the delegated authorities by correcting wrong decisions as may be necessary, up to the point of revocation.

A principal question for the subject of this paper is the correlation between regulation and deregulation in the communication industry. As was demonstrated, it is now almost completely within the scope of state regulation primarily focused at prices and tariffs for communication services. There is a goal to phase out state regulation of tariffs in competitive sectors, a process to be underpinned by analysis of implications of deregulation in respect of specific natural monopolies[14]. In other words, a legal experiment should be conducted on whether it is feasible to abandon state regulation of tariffs. Developing an infrastructure available to a wide range of market players will also set the stage for the promotion of competition and thus for relaxing or terminating state regulation of tariffs.

Some steps in this direction are already being made. Thus, Federal Law "On Communication" has come to include Article 53.1 "Provision of information under the programme of experimental legal regimes in the sector of digital innovations" (introduced by Federal Law No. 331-FZ of 02 July 2021) whereby in accordance with the said programme approved by Federal Law No. 258-FZ of 31 July 2020 "On the Experimental Legal Regimes in the Digital Innovations Sector in Russia" mobile Telecom operators as par-

[14] FAS of Russia Order No. 279/18 of 12 March 2018 "On Approving a FAS Action Plan to Implement the 2018-2020 National Plan for the Promotion of Competition in the Russian Federation approved by Presidential Decree No. 618 of 21 December 2017 "On the State Policy Guidelines for the Promotion of Competition"// SPS Consultant Plus.

ties to the experimental legal regime were granted broader rights including those to pass to their peers the information on the number of subscribers located in the given period in a territory covered by such regime. Obviously, the opportunities related to human rights could be settled only at the legislative level and exclude any self-regulation.

While the availability of alternative communication services is positive for the market development, it does not affect the extent of state regulation of those services are already covered by the regulatory scope. However, the industry is rapidly developing, with new communication technologies and services making their appearance. As a result, new services are not as regulated as the traditional communication services for a certain period of time. This, however, does not mean zero regulation since these relationships are governed by provisions of the Civil Code. As an option for further regulatory development, there is a scope for broader coverage of the existing communication services by the Civil Code.

Communication services are hard to separate from telecommunications such as Internet access services. As regards this group of relationships, it can be asserted that the scope of state intervention is ever increasing largely due to the efforts to counter illegal or harmful content and terrorism and to ensure information security. This, however, affects the interests of telecom operators who assume extra duties. For example, a resolution on the rules for identification of users of messenger apps effective since 05 May 2019 was passed by the Federal Government as a result of amendments to the Federal Law "On Information, Information Technologies and Data Security" whereby organizers of an instant message exchange service should accept messages only from identified users, with system administrators required to refer to telecom operators for user details. The extra duties of telecom operators also follow from statutory requirements to ensure local residency of personal data, storage of connection data, protection of proprietary rights etc. The legal status of Telecom operators can be specified only by regulation including with the purpose of imposing extra duties.

Conclusion

It has to be admitted that the communication industry is largely regulated by the state, with the trends for deregulation visible only as regards pricing. However, some issues important for both the Government and

businesses, primarily those of security, require concerted efforts. Here the Government should exercise statutory regulation by leaving to economic agents the choice of the most optimal means of protection, identification of security requirements, development of security policies etc. The fight against child pornography, safe Internet initiatives etc. promoted not only by regulatory means but also by private action could come within the scope of concerted efforts of the Government and Telecom operators.

References

1. Administrative procedures and control in light of European experience (2011) T.Ya. Khabrieva, J. Marcou (eds.). Moscow: Statut, 320 p. (in Russ.)

2. Baumann S. (2005) *The individualized society.* Moscow: Prospekt, pp. 27, 53–54 (in Russ.)

3. Digital transformation and public governance (2022) A manual. Moscow: Infotropik Media, 224 p. (in Russ.)

4. Discretion and taxation (2017) Comments to tax administration law and practice. SPS Consultant Plus (in Russ.)

5. Dyomin A.V. (2017) *Soft law in the times of changes: a comparative study.* Moscow: Prospekt, 240 p. (in Russ.)

6. Gubin E.P. (2022) Sustainable development of the market economy and private enterprise: legal aspects. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 1, pp. 36–46 (in Russ.)

7. Kovalev A.A. (2013) International protection of human rights: textbook. Moscow: Statut, pp. 115–116 (in Russ.)

8. Krasinsky V.V. (2017) *The protection of state sovereignty.* Moscow: Norma, 608 p. (in Russ.)

9. Kucherov I.I., Sinitsyna S.A. et al. (2022) Digital economy. Relevant areas for regulation: a guide. Moscow: Norma, 376 p. (in Russ.)

10. Markvart E., Kurbanov B. (2018) Different from others: bankruptcy law applied to public law entities and public companies: the case of Germany and Russia. *Imuschestvennye otnosheniya v Rossii*= Property Relations in Russia, no. 6, pp. 61–78 (in Russ.)

11. Morozova L.A. (2002) The theory of state and law: textbook. Moscow: Statut, 288 p. (in Russ.)

12. Nerseyants V.C. (2001) The general theory of state and law. Moscow: Norma, p. 489 (in Russ.)

13. Novoseltsev A.Yu. (2022) The issue of concluding international convention on foreign investments. *Miezhdunarodnoye publichnoe i chastnoe pravo*=International Public and Private Law, no 1, pp. 10–13 (in Russ.)

14. Nozdrachev A.F. et al. (2015) Permitting system in the Russian Federation: a guide for research and practice. Moscow: INFRA-M, 928 p. (in Russ.)

15. Romanovskaya O.N. (2017) Delegating governing powers in the public law regulation system. *Vestnik Permskogo gosudarstvennogo Universiteta*. *Yuridicheskiye Nauki*=Perm State University Bulletin. Law Sciences, no. 2, pp. 143–154 (in Russ.)

16. Statutory regulation of economic relationships: textbook (2018) E.P. Gubin, S.A. Karelina (eds.). Moscow: Statut, 256 p. (in Russ.)

17. Tikhomirov Yu.A. (1994) *Governing affairs of the society.* Moscow: Yuridicheskaya literatura, pp. 193–213 (in Russ.)

Information about the author:

L.K. Tereschenko — Honorary Lawyer of Russia, Senior Researcher, Doctor of Sciences (Law).

The article was submitted to the editorial office 15.11.2022; approved after reviewing 30.11.2022; accepted for publication 30.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Research article
УДК: 342
DOI:10.17323/2713-2749.2022.4.67.87

Transformation of E-Government and E-Governance in the Digital Economics

Nikita Arkadievich Danilov

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia, ndanilov@hse.ru, ORCID: 0000-0003-4924-202X

Abstract

The article deals with the development issues of e-government and e-governance in Russia and elsewhere. In modern society the social relationships appeared to be as evolving under the notable impact of information and communication technologies. The functioning of the state also changes in a number of aspects, with all three branches of governance affected by transformations. Executive authorities are subject to the most significant changes. With the emergence of e-government in countries with different political and legal traditions, the procedure for the provision of public and municipal services is changing and executive authorities become more transparent. The ongoing processes have to be theoretically studied including with the purpose of developing a comprehensive approach to regulation of e-government. In this regard, it is necessary to take into account and analyze the international experience of building e-government as well as the general and specific features of the applicable law. The focus of the study is e-governance and executive branch in the context of information society — in particular, the legal provisions applicable to e-government as a new state of executive authorities in Russia and internationally. It has been found in the course of the research that the development of e-government is followed by transformation of the system of executive authorities, with supra- and interagency bodies emerging to coordinate the action of other executive bodies for managing the affairs of information society, develop the concerted policies and also supervise other executive bodies amid the centralization of e-government powers and development of e-government.

Keywords
transformations; e-government; e-governance; digital governance; executive authorities; public services.

For citation: Danilov N.A. (2022) Transformation of E-Government and E-Governance in the Digital Economics. *Legal Issues in the Digital Age,* vol. 3, no. 4, pp. 67–87. DOI:10.17323/2713-2749.2022.4.67.87

Background

The emerging information society requires common information space to be created through concerted public policies and coordinated governance by executive authorities. In this regard, the state machinery undergoes a transformation, with special supra-agencies being created to pursue consolidated information policies and coordinate action of other executive bodies for managing the affairs of information society. In addition, interagency bodies spring up to coordinate action of other executive bodies. Unlike other executive bodies of the sectoral competence, these supra- and interagency bodies have intersectoral competences which allow them to introduce provisions and exercise powers in respect of different executive bodies in connection with different areas of regulation (such as access to information, public e-services, personal data protection, etc.). These bodies also have the power of control in respect of other executive bodies.

Under the internationally adopted politico-legal doctrine, a distinctive feature of e-government is the emergence of interagency commissions to focus on general tasks. These commissions normally handle the administrative aspects of the development of e-government: they will decide what should be done or changed in the operational arrangements of executive bodies to improve the e-government. The following factors determine whether such interagency bodies are good: clearly defined interagency powers, reporting to a supreme executive body or specially created government committee responsible for the development of e-government; appointment of senior officials from the executive branch — ideally not below deputy minister — to the commissions (so that they can adopt binding decisions); clear coordination of action between commission members and executive bodies; powers to take decisions and/or propose recommendations to the supreme executive body for the development of e-government;

possibility to participate in the allocation of budget funds for development of e-government or to issue instructions to the financial authorities on desirable spending of funds.

A need to pursue consolidated information policies can be attributed to the nature of information space as a multi-faceted and at the same time holistic phenomenon. Whereas in the past the executive bodies would operate strictly within the powers afforded to them, the situation changes in the context of information society since managing the affairs of a complex social phenomenon will require that public bodies develop cooperation between them and that certain supra- or interagency bodies assume the powers for the development of e-government and for control of executive bodies' compliance with individual rights of access to information and public e-services.

As was rightly noted by I.L. Bachilo with regard to a manifestation of the observed trends, "it can be assumed that the supervisory structures will become more consolidated, with the emergence of control bodies beyond the scope of each ministry" [Bachilo I.L., 2005: 17]. Meanwhile, the trend for the executive reform is much wider: new supra- and interagency bodies not only assume control powers but also exercise statutory regulation, develop public policies for the promotion of e-government, and coordinate action of other executive bodies.

1. E-Government and the Transformation of E-Governance in Russia

In Russia, the Ministry of Digital Development, Communication and Mass Media (MDD) is in charge of E-Government.

Under Federal Government Resolution No. 418 of 02 June 2008 "On the Ministry of Digital Development, Communication and Mass Media", the MDD is a federal executive agency for "the development and implementation of public policies and regulation in the area of information technologies (including IT used to put in place and provide access to public information resources), and the provision of public IT services including IT which is used to put in place and provide access to public information resources"[1].

[1] SPS ConsultantPlus.

The MDD is also the federal executive agency authorized to regulate the use of e-signature. Its regulatory scope includes the identification of individuals based on biometric personal data and the development of requirements to the format of data used in public information systems.

The Ministry ensures "the availability of information systems for the public service provision in a proactive way including via the integrated portal of public and municipal services/functions, integrated identification and authentication system based on automatic receipt of the required data from data systems (including public data systems) or resources (including public resources), in particular, those on civil registration to be provided by the integrated state register of births, deaths and marriages"[2].

The MDD has a number of powers regarding the development of e-government and E-Governance in Russia with the following priority areas being identified: development of information government (government-wide/regional IT penetration, digital transformation of public agencies); development of E-Government (e-services for individuals/businesses, e-government infrastructure, integrated biometric system, superservices, as well as digital transformation of public services); nationwide digitization (coordination, monitoring and implementation of the regional digitization, digital transformation strategies).[3]

Thus, the MDD is responsible for coordination of digital transformation as well as development of E-Governance in other public agencies including both federal and regional executive bodies.

To conclude, the Ministry is a kind of "supra-agency" responsible for development of e-government as a whole.

This approach has resulted in the fast and efficient development of E-Government in Russian Federation. The country traditionally ranks fairly high in the United Nation's e-Government Development Index (EGDI), which is one of the key development indicators of information society and digital governance worldwide.

In 2022, "Russia ranked 42nd among 193 countries (36th place two years before). Russia is ahead of the countries such as Croatia (44), Czech

[2] SPS ConsultantPlus.

[3] Available at: URL: https://digital.gov.ru/ru/activity/ (accessed: 22.11.2022)

Republic (45) … and Slovakia (47)"[4]. Russia's EGDI index "fell 0.008 point over two years down to 0.8162"[5].

This result is anyway considerably higher than the global average of 0.61 point. As a matter of comparison, "Denmark ranks first with 0.97 point while South Korea leading in Asia has 0.95. Kazakhstan has maintained its leadership in Central Asia in terms of e-government development with 0.86 point in 2022 against 0.83 two years before"[6].

Thus, a relatively small number of points to be earned will get Russia to the top of the list which is quite feasible in view of the progress achieved by the MDD and Federal Government in digitizing the state machinery and public services.

Apart from the MDD, there is the Governmental Commission for Development of Information Technologies for Improvement of Living Standards & Business Environment (hereafter –"Commission"). The Commission is "a steering body established to ensure cooperation between the federal executive authorities and local governments to develop the ecosystems of digital economy and to promote the use of IT and communications in general for the benefit of information society and e-government in Russia".[7]

As follows from the Government of the Russian Federation Resolution No. 1065 of 07 September 2018, Commission mentioned is charged with the following main tasks: promoting the use of IT for better quality and accessibility of public and municipal services available to individuals and legal entities; organizing public bodies for international cooperation regarding IT and improvement of Russia's information technologies development ratings.

The Commission's presidium mainly deals with steering the government efforts at the federal and regional levels to design consolidated public policies for development of digital platforms for the benefit of economic sectors including public administration and municipal economy; develop-

[4] Available at: URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D0%B5%D0%B9%D1%82%D0%B8%D0%BD%D0%B3_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%B0_%D0%9E%D0%9E%D0%9D_(EGDI) (accessed: 22.11.2022)

[5] Ibid.

[6] Ibid.

[7] Available at: URL: http://government.ru/department/492/about/ (accessed: 22.11.2022)

ment and use of IT and digital platforms, and development of a modern information and communication infrastructure; better performance of the budget expenditures for IT penetration and use by public authorities; decision-making to put in place and use an infrastructure for data exchange and technological interaction between data systems used for the provision of public and municipal services and performance of public and municipal e-functions; transition towards public and municipal e-services; development of a consolidated identification and authentication system to be integrated into federal, municipal and other data systems for provision of public, municipal and other services; coordinated development of interagency data exchange and integration of public, municipal and other data systems for provision of public, municipal and other services; decision-making for public data management and transfer to the analytical data support subsystem of the federal public information system "Universal information platform of the national data management system".

The Commission is headed by the Chairman of the Russian Federation Government who leads its activities and is responsible for achievement of the tasks assumed by the Commission.

The Commission includes, apart from the Chairman of the Government, a Deputy Chairman responsible for coordination of federal executive agencies with regard to digital transformation of governance, digital development and public policies in the area of communication, as well as the executive secretary and other members.

The Commission also includes representatives of different federal executive bodies and government-funded entities.

Thus, Russia has a "supra-agency" governmental commission for the development of e-government and digital governance, and coordination of relevant activities of federal executive bodies. While this commission does not have the status of a public agency, its high level makes its decisions and instructions binding on federal executive bodies.

2. Centralization of Functions and Services of the Business Sector

Apart from centralization of e-governance functions in Russia, there is a trend to set the stage through legislative reform for centralization of business activities in the sector of digital services and technologies.

Thus, before the e-signature law was reformed in 2019, there were 322 certification centres in Russia authorized to issue enhanced qualified e-signatures. Such a large number of certification centres actually made supervision impossible, only to result in more cases of fraud where, for example, a centre could issue an enhanced qualified e-signature for an illegal real estate transaction.

Federal Law No. 476-FZ of 27 December 2019 "On Amending the Federal Law on E-Signatures and Article 1 of the Federal Law on Protection of the Rights of Legal Entities and Private Entrepreneurs Subject to Public Control/Supervision and Municipal Control"[8] has introduced considerably tighter requirements to certification centres which are deemed to include the accredited centres as well as the certification centre of the federal executive agency for state registration of legal entities (FTS of Russia), the certification centre of the federal executive agency for enforcement of the federal budget execution and for cash services for the execution of budgets of the Russian budgetary system (Federal Treasury), as well as the certification centre of the Central Bank of Russia.

This is one more example of the centralization of digital services and functions, with public authorities assuming in fact a preemptive right to issue key certificates for enhanced qualified e-signatures instead of "commercial" certification centres (those privately owned outside the system of public agencies or institutions). Moreover, the Federal Law "On E-Signatures" was amended for tighter requirements to the accreditation of "commercial" certification centres, with just about 30 of those previously in existence being accredited as the amendments took effect.[9] These were often the certification centres of large banks or nationwide telecom operators.

The centralization of functions and services for (biometric) identification of persons is another example. In simple terms, biometric identification is a system for identification of people by their unique physical parameters with the purpose of performing transactions or other legally binding actions. The biometric identification can be used for access to an ATM, opening or making transactions in a bank account/deposit, shopping, accessing the restricted areas etc. For the personal data to get to the

[8] SPS Consultant Plus.

[9] Available at: URL: https://digital.gov.ru/ru/activity/govservices/2/?utm_referrer=https%3a%2f%2fwww.google.com%2f (accessed: 22.11.2022)

biometric identification system, the person in question should make his or her reference details (face image, voice print, finger prints etc.) available to the system operator.

The Federal Law "On Information, Information Technologies and Data Protection" defines the identification as "a set of interventions to establish and verify personal details in accordance with federal laws and the underlying regulations, and to compare the said details with the unique designation(s) of personal details required to identify such a person (identifier)".[10]

This definition is not quite adequate as it makes, for example, the passport number and series a unique identifier. Will a comparison of someone's personal details (photo and full name) with the passport number/series identify a person? The answer to this question is obviously no.

What makes this definition still more problematic is that the identification procedure could be in fact established exclusively by "federal laws and the underlying regulations". This means that the identification procedure cannot be agreed between the parties, only to question the use of different identifiers developed and introduced by non-governmental entities (such as banks, telecom operators, Internet providers etc) to perform transactions and other legally binding actions.

Based on his experience of the Digital Environment of Confidence working group under the Competence Centre for Statutory Regulation of the Digital Economy (Skolkovo Fund), the author would propose the following terminology developed with participation of other members. A personal identifier is the unique designation of personal details in an information system or database required to identify a person through the use of technical and/or technological methods. Identification of a person is a set of interventions to specify personal identifiers and other details to be performed under the law and/or by agreement between the parties. Personal authentication is a process to confirm that the identifier(s) belongs to a person by way of comparing it with the available details and thus to prove the identity of the previously identified person.

Before the 2020 reform of biometric identification, different organizations — first of all, banks — would develop "proprietary" biometric systems[11].

[10] SPS ConsultantPlus.

[11] Available at: URL: http://www.sberbank.ru/ru/person/dist_services/bio (accessed: 22.11.2022)

However, Federal Law No. 479-FZ of 29 December 2020 "On Amending Specific Regulations of the Russian Federation"[12] established that biometric identification should be performed in Russia primarily through the use of a universal biometric system (UBS) as a public information system.

Under the new requirements, it was generally forbidden to financial market agents and other organizations and private entrepreneurs to collect and process biometric personal data in their data systems with the purpose of identification and/or authentication, except in cases provided for by law and for depositing with the UBS under federal law.

Financial market agents and other organizations may collect and process biometric personal data in their data systems with the purpose of authentication where the following conditions are simultaneously met:

such organizations have made the administrative and technical arrangements for security of personal data, and have applied the data protection technologies for protecting personal data from threats;

the individual has agreed to have his or her biometric personal data processed for the stated purpose including in the interest of a specific third party;

such organizations have been accredited.

Financial market agents and other organizations may be allowed to collect and process biometric personal data in their data systems for identification and authentication in cases established by the Federal Government in coordination with the Central Bank of Russia where simultaneously:

the aforementioned requirements have been met;

the requirements of the Federal Law "On Information, Information Technologies and Data Protection" and the Federal Law "On Security of the Critical Data Infrastructure of the Russian Federation" have been met;

the individual has agreed to have his or her biometric personal data processed for the stated purpose including in the interest of a specific third party;

such organizations have been accredited.

Where in the process of collecting and processing biometric personal data under the federal law the financial market agents and other organizations have collected biometric personal data compatible with the UBS data

[12] SPS ConsultantPlus.

in terms of quality and other requirements, such data are to be deposited with the UBS upon consent of the individual in question.

The last requirement to "proprietary" biometric identification systems is remarkable as it essentially means that system operators are required to make "quality" biometric data available to the UBS. Is this legislative solution justified in terms of security of sensitive biometric data, improvement of the procedure for use of biometry, extension of the UBS scope? Does it amount to "digital nationalization" unprecedented in human history where business entities that have invested into the creation and development of their own systems for data identification and collection will have to deposit commercially valuable data to a public data system on a centralized basis? This will apparently become clear in one or two years from the effective date of the amendments, once the practice of enforcement is there.

Also, under Federal Law No. 479-FZ of 29 December 2020 "On Amending Specific Regulations of the Russian Federation", the identification of a physical person should be performed by establishing and/or confirming his or her personal details by comparing the personal data provided by the relevant organization's data system with those maintained by the UIAS and also by using the information on whether the provided biometric personal data is compatible with the data maintained by the UBS, or, where the UBS does not have such data, with those of a proprietary biometric system. Thus, the data used in such system will have to be compared with those maintained by the UBS even where a proprietary system for biometric data identification is involved.

The legislator has established strict requirements to the use of proprietary biometric data identification systems and required such proprietary data to be additionally checked by the UBS by demanding that proprietary systems deposit with the UBS *quality* duplicate data. Once implemented, the new requirements will actually result in the centralization of functions and services for biometric personal identification.

3. Transformation of E-Government and E-Governance in the United States and continental Europe

In the United States, the Office of E-Government will act as a supra-agency body responsible for the e-government function, with the highest authority to be assumed by the Administrator. The Office was established

under the Office of Management and Budget. Since the Office of E-Government has the right to define the rules for all executive bodies and supervise their compliance with the established requirements, it can be concluded that this body has supra-agency functions.

As a peculiar feature, the US E-Government legislation details the legal status of supra-agency and interagency bodies responsible for the development of e-government. In the United States, the structural changes to the government machinery are enshrined at the legislative level.

Under the E-Government Act of 2002[13], the E-Government Office Administrator is charged, in particular, with planning and controlling the investments into IT technologies, ensuring information security and personal data protection, making the information on the government activities publicly available, disseminating and safeguarding the information on the government activities, and also ensuring access to IT technologies to persons with disabilities.

As regards development, the Administrator will advise senior government officials on issues relevant to e-government efficiency. The Administrator has to propose changes to the strategy and priorities of e-government, exercise the general direction of executive bodies for development of e-government, and identify the guidelines. The Administrator has to promote the innovative use of IT technologies by executive bodies. In particular, he is supposed to encourage interagency collaboration. The Administrator will control the allocation and targeted use of funds earmarked for the development of e-government.

This officer will coordinate the implementation of programmes for development of e-government and efficient use of IT technologies by the executive branch. He will help senior executives to establish the standards to be applied by the Federal Government to IT technologies. These standards concern the following aspects: network interaction and IT compatibility; efficient IT use by the Federal Government; security of computer systems used by public authorities.

The Administrator will coordinate the work of the executive branch for development of e-government. He has the duty to arrange for the relevant discussions between senior officials of the Federal Government, state gov-

[13] Available at: https://www.justice.gov/opcl/e-government-act-2002 (accessed: 21.11.2022)

ernments, tribal authorities, representatives of the executive, legislative and judicial branches, as well as senior executives of private and no-profit sectors with the purpose of promoting cooperation and wider use of the best innovative approaches in using and managing information resources. These discussions also purport to ensure better use of IT technologies by the government for more adequate provision of information on government activities and improvement of the public service provision.

Apart from the general direction of the executive branch in respect of e-government development, the Administrator also has the power of control over all executive bodies. He will exercise control over executive bodies on the way they implement and use the integrated information system and supervise the development of information infrastructure used by executive bodies both at the intra- and interagency level. The Administrator will assist senior government officials to make sure the executive bodies apply adequate, risk-weighted and economically efficient safety measures in developing e-government.

As was demonstrated above, the Office of E-Government is a supra-agency body. It can issue instructions binding on executive bodies in relation with the development of e-government, exercise general direction and coordination of the executive branch, and has the power of control. Apart from the Office, the E-Government Act of 2002 provides for the creation of an interagency body for teaming up different executive bodies relevant to the development of e-government in the United States.

Such interagency executive body vested with e-government related powers is the Chief Information Officers Council that includes senior officers of a number of executive bodies such as deputy head of the Office of Management and Budget (Council Chairman), E-Government Office Administrator (Deputy Chairman), Administrator of the Office of Information and Regulatory Affairs, senior officer of the Central Intelligence Agency for implementation of information policies, senior officers of the Army, Navy and Air Force Departments responsible for information policies, as well as relevant officials of a number of other executive bodies. The Council may also include other officials as appointed by the Chairman of this interagency body.

The Council aims at improving the performance of the executive branch as regards the deployment, purchase, development, upgrading, use, operation and accessibility of the federal information resources.

In performing its functions, the Council is expected to hold regular consultations with representative bodies of the States as well as with the local governments and tribal authorities. Under the US law, the Council is vested with the following powers: making proposals for the improvement of governmental information resources; exchanging the best practices, ideas, methods and innovative approaches related to managing information resources; assisting the E-Government Office Administrator to identify, develop and coordinate interagency projects and other innovative initiatives for the use of information resources by the Government; encouraging public agencies to develop and use interagency programmes for managing information resources.

Apart from the centralized management of e-government development, the U.S law also provides for the centralized distribution of relevant funds.

Thus, the E-Government Act provides for a special E-Government Fund to be set up in the US Treasury Department and used to support the projects enabling the Federal Government to build up its capabilities (by way of developing and introducing innovative methods of using the Internet and other IT technologies) for performance of functions. The projects financed by the Fund should pursue the following objectives: making the Federal Government information and services more readily available to members of the public (including individuals, businesses, State and local government); facilitating the access to services and information of and transactions with the Federal Government; enabling the federal agencies to take advantage of information technologies in sharing information and conducting transactions with each other and with State and local governments.

As a peculiarity of e-government regulation in the United States, the law provides for the duties of executive bodies to develop e-government, with their senior officers to be held liable for a failure to comply with the established requirements.

It is provided that the heads of the executive branch are responsible for compliance with the requirements of the E-Government Act and for adequate information management as well as for compliance with the rules issued by the Office of E-Government. The heads of executive bodies are required to advise public servants on the established requirements and rules. They are required to assist the Office of E-Government to develop,

support and promote integrated web systems for the provision of Federal Government information and services to the public.

The executive branch is required to take steps for the assessment of performance of e-government and for control of whether the relevant activities comply with the objectives and powers of public bodies.

The assessment exercise should rely on the following criteria: standards of services provided to members of the public; public agency's performance; innovative information technologies introduced.

The executive bodies should cooperate with each other as far as possible to develop the collective objectives and to collectively use information technologies for the provision of public services and information.

As was said above, the Office of E-Government has the power of control over other executive bodies, with the latter correspondingly obliged to draft and submit to the Office an annual report on the promotion of E-Government. The report should include the details of the agency's initiatives to promote E-Government, information on compliance with the E-Government Act and also on how the E-Government promotion initiatives resulted in the provision of better services and information.

Thus, the statutory regulation of E-Government in the United States is an illustrative demonstration of structural changes of the executive government system in the context of information society. For the effective E-Government capability, the government has to set up bodies with a special status vested with supra-agency and interagency functions. This is necessary for a concerted action of public authorities, for control of their compliance with e-government development requirements, and for uniform enforcement practices.

The structural changes to the executive government system are less visible in other countries where information commissioners or sectoral ministries (for communication, IT etc.) will normally assume certain functions for the development of e-government. These bodies develop regulations applicable to the relationships for the provision of information and e-services by the executive branch. Moreover, they have noticeably fewer functions than the Office of E-Government and the Chief Information Officers Council. This can be due to the fact that "E-Government" as a term and its statutory regulation first emerged in the United States. Obviously, it will take certain time from the moment the e-government is established before the executive gov-

ernment system undergoes major structural changes induced by the special status bodies. It is a well-known fact that the E-Government concept started to develop in the United States earlier than elsewhere.

Unlike the United States, the countries of continental Europe do not envisage to set up agencies endowed with a broad range of powers for regulation of access to information and services. Their laws will normally identify the bodies responsible for "bottlenecks" in statutory regulation of information relationships. They set up standalone executive bodies for public policy development and statutory regulation, development of public e-services, protection of personal data of individuals, as well as those charged with development of telecommunication networks in their national territory. Thus, the countries of continental Europe, once more unlike the US, do not envisage to set up any supra-agency bodies within the executive branch or interagency commissions responsible for the development of E-Government.

One exception is Italy, which has adopted the E-Government Code for a structural transformation of the government machinery by a special executive body (Digital Policy Agency[14]) responsible for better use of IT technologies by the executive branch. The Agency will pursue public policies for the development of E-Government, participate in the implementation of public infrastructure projects, and take steps to promote an integrated public system for e-communications and cooperation. The said system is a technological network designed for a concerted public service provision by executive authorities. The Agency will provide technical support and advise the executive branch and the Council of Ministers of Italy on issues related to the development of e-government.

Moreover, Italy's executive agencies and their subdivisions are required to develop and implement e-government development projects within their respective competence.

To establish a common information space, Italy has put in place a public system for collaboration between public and municipal bodies which integrates the networks of local, regional and central government agencies into one system governed by universal security and quality standards. In addition, there is an international public network which provides connectivity to more than 540 overseas representation offices of the Italian government.

[14] Available at: http://www.digitpa.gov.it/ (accessed: 22.11.2022)

This system is used, in particular, to handle registration transactions outside the national territory.

Thus, unlike a number of other countries where interagency e-cooperation systems are used by executive bodies primarily to exchange information and documents only for the public service provision, the Italian system for electronic cooperation between public and municipal bodies has a much wider scope.

The system is used for exchanging any kind of information and documents as well as for coordinating a concerted action of the executive branch. It covers all public and municipal bodies plus representation offices of the Italian government outside the national territory. Public agencies are required to exchange messages electronically (by e-mail). The data stored by one public agency should be accessible to any other public agency. Where public bodies are required to cooperate for a specific public function (licensing, permissions, regulation of public works), an e-conference involving public servants from a number of agencies will be convened. Online conferences serve to minimize financial and time costs of the public authorities.

Irrespective of the statutory powers provided for the development of e-government, the executive bodies in countries of continental Europe can be divided into several groups.

The first group covers the executive bodies authorized to regulate the procedure for e-service provision.

Thus, for example, Austria's E-Government Act of 2004[15] envisages setting up a registration agency authorized to assign identification numbers to individuals and to issue "citizen cards".

The second group includes the bodies with regulatory powers authorized to control whether executive bodies observe confidentiality provisions with regard to personal data available to them.

In Denmark, the Data Protection Agency set up specifically under the Personal Data Protection Act of 2018[16] is charged to supervise compliance with personal data protection law (including by public authorities).

[15] Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://joinup.ec.europa.eu/sites/default/files/document/2015-03/egov_in_austria_-_january_2015_-_v_18_0_final.pdf (accessed: 22.11.2022)

[16] Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (accessed: 22.11.2022)

The Data Protection Agency is authorized to monitor all personal data processing operations (outside the supervisory powers of courts). The exception established by law is based on the concept of separation of powers whereby an executive body is not authorized to issue statutory instruments and regulations binding on judiciary bodies. The Agency, by its own initiative or on the basis of complaints filed by data subjects, will exercise control to make sure that executive bodies process personal data in compliance with provisions of personal data protection law.

Thus, in countries of continental Europe there are normally no supra- or interagency authorities with a special status responsible for E-Government but only specific executive bodies (or specifically authorized bodies already in existence) with a sectoral competence for the promotion of E-Government. While some agencies have the powers to regulate and supervise public e-services provided by other executive bodies, others perform regulatory functions for control of compliance with personal data protection rules.

Conclusion

Closer cooperation between public agencies in the context of IT technologies, with new executive bodies vested with supra-agency powers being set up, is characteristic of a number of countries, including Russia, that develop E-Government. This trend prompts some researchers to draw a quite radical conclusion (at the first glance) that the traditional hierarchy of public bodies with sectoral competences and structural subdivisions (offices, departments) headed by a sole manager (minister, director etc.) will be gradually ousted by the bodies with interagency competences covering those of a number of public authorities.

Close cooperation indicative of a trend for the emergence of bodies with interagency clout is due not only to the adoption of necessary regulations but also to objective reasons, of which the most important is the creation of government-wide web portals which allow public bodies to collectively provide public services, something that requires cooperation between themselves and their structural subdivisions, joint consultations and development of joint administrative procedures for the service provision.

Under E-Government model of present days, the Government-wide portal is supposed to be used for public service provision and access to information on the activities of executive bodies. The creation of such portals

will involve cooperation between executive bodies as well as development of universal technological standards and adoption of provisions on data security and compatibility of software used by different agencies. Government-wide portals for the public service provision were first established in countries such as Canada, Singapore, Hong Kong and France [Allen B., Juillet L., Paquet G., Roy J., 2005: 3]. Other countries promoting E-Government follow in their wake — including the Russian Federation that has now an integrated portal for public and municipal services.[17]

It is yet premature to speak of a "merger" of executive bodies to result in agencies for control over several sectors at a time. However, a trend for creation of steering bodies to team up the executive branch for the promotion of E-Government institutions such as Government-wide public service portals has become widespread in common law countries, with other countries expected to follow suit.

Closer cooperation between executive bodies to create government-wide portals for public services and develop integrated service packages is typical of the last (fourth) stage of the development of E-Government.

While the classic model of government machinery endows executive bodies with a significant extent of autonomy and independent decision-making, E-Government will blur a good many lines.

The use of IT technologies by the executive branch results not just in the emergence of agencies with a special status and in simplification of their activities but also in stronger links between different bodies.

Executive bodies electronically coordinate their service provision to result in a kind of "integration" of public services to be provided with the involvement of several agencies at a time [Nixon P., Koutrakou V. et al., 2010: 62, 100]. Coordination may be carried out both by executive bodies of equal rank ("horizontal" coordination) and by hierarchically subordinated bodies ("vertical" coordination).

Closer cooperation between executive bodies can be attributed to a desire to satisfy the needs of individuals. While individuals normally seek information on a specific issue, their requests may involve processing the information available to different bodies in order to be satisfied. Thus, ex-

[17] Available at: URL: http://www.gosuslugi.ru/ (accessed: 22.11.2022)

ecutive bodies have to coordinate their efforts for a full-fledged "comprehensive" response [Hague B., Loader B., 2005: 82].

In the context of progressing information technologies executive bodies have the capability of interrelated service provision, something that gradually forces them to standardize their administrative procedures and develop cooperation with each other [Holmes D., 2001: 59].

As observed in the USA E-Government Act, most Internet-based services of the Federal Government are developed and presented separately according to the jurisdictional boundaries of executive agencies rather than being integrated for a streamlined provision. In this regard, the purpose of the Act is to promote interagency collaboration for provision of e-services and to integrate related executive functions.[18]

Thus, as was demonstrated above, the development of E-Government is paralleled by transformation of the executive branch.

Remarkably, the United States have a supra- and an interagency body responsible for promotion of e-government, development of public policies, statutory regulation and supervision of other executive bodies for provision of public e-services and disclosure of information on activities of the executive branch. That the most significant changes in the executive government system have occurred in the United States can be attributed to the relatively early development of the E-Government concept in this country as compared to others. The evolution of E-Government in the United States has prompted a need in the centralized approach to statutory regulation and resulted in a special legal status afforded to the Office of E-Government and to the Chief Information Officers Council under the act which defines the legal and institutional basis of e-government.

A wide range of powers afforded to the MDD of Russia also suggests that this body, in spite of its equal rank with other federal bodies, is vested

[18] An example of promoting interagency cooperation for provision of public e-services is Arizona. This state has put in place the Right Door Program to integrate more than 150 social security programmes provided by 5 agencies, with a single portal to be used irrespective of the agency to be involved in social security provision. Social security agencies collectively develop and maintain an information system from which individuals may learn whether they qualify for social assistance and apply for it.

Thus, instead of referring to a specific agency for each specific service, individuals may use the integrated system and receive simultaneously several types of social security to be provided by different agencies.

with supra- and interagency jurisdiction in respect of digitization of government and promotion of E-Government.

Other countries will set up bodies endowed with sectoral competences regarding the development of E-Government. These are normally sectoral ministries or commissioners for the protection of information access rights specifically authorized to develop the public service provision, regulate and control the access to information on government activities. As a general trend, such bodies will be set up primarily in countries with the parliamentary political regime.

Since the development of E-Government requires a concerted and coordinated action by all of the executive branch machinery, the emergence of supra- and interagency bodies is likely to become a characteristic feature of other countries seeking to promote E-Government.

References

1. Allen B., Juillet L., Paquet G., Roy J. (2005) E-Government as Collaborative Governance: Structural, Accountability and Cultural Reform. In: Practicing E-Government: A Global Perspective. Hershey: Idea Group Publishing, 457 p.

2. Bachilo I.L. (2005) Information Issues in Public Governance. In: Information Issues of Administrative Reform. Collection of essays. Moscow: Norma, pp. 8–23 (in Russ.)

3. Digital Democracy. Discourse and Decision-Making in the Information Age (2005) B. Hague, B. Loader (eds.). L.: Taylor and Francis Group, 294 p.

4. Digital Democracy: Issues of Theory and Practice (2001) K. Hacker, J. Dijk (eds.). Thousand Oaks: SAGE Publications, 240 p.

5. Evans D., Yen D. (2006) E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, no. 23, pp. 207–235.

6. Henman P. (2010) *Governing Electronically. E-Government and the Reconfiguration of Public Administration, Policy and Power.* N.Y.: Palgrave Macmillan, 489 p.

7. Ho T. (2002) Reinventing Local Governments and the E-Government Initiative. *Public Administration Review*, no. 62, pp. 434–444.

8. Holmes D. (2011) *E-Governance. E-Business Strategies for Government.* Naperville: Nicholas Brealey Publishing, 165 p.

9. Homburg V. (2008) Understanding E-government. Information Systems on Public Administration. L.: Taylor and Francis Group, 512 p.

10. Jaeger P. (2005) Deliberative Democracy and the Conceptual Foundations of Electronic Government. *Government Information Quarterly,* no. 22, pp. 702–719.

11. Lasifidis P., Nicoli N. (2001) *Digital Democracy, Social Media and Disinformation*. L.: Taylor and Francis Group, 345 p.

12. Malkia M., Anttiroiko A., Savolainen R. (2004) *E-Transformation in Governance: New Directions in Government and Politics.* Hershey: Idea Group Publishing, 338 p.

13. Pavlichev A., Garson G. (2004) Digital Government: Principles and Best Practices. Hershey: Idea Group Publishing, 309 p.

14. Understanding E-Government in Europe: Issues and Challenges (2010) P. Nixon, V. Koutrakou et al. (eds.). Abingdon: Routledge, 352 p.

15. West D. (2007) *Digital Government: Technology and Public Sector Performance.* Princeton: Princeton University Press, 256 p.

Information about the author:

N.A. Danilov — Associate Professor, Candidate of Sciences (Law).

The article was submitted to the editorial office 07.11.2022, approved after reviewing 30.11.2022, accepted for publication 30.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.
Research article

УДК: 342.34
DOI:10.17323/2713-2749.2022.4.88.105

E-Democracy: A Constitutional Dimension

Albina Slavovna Lolaeva

Gorskiy State Agrarian University, 37 Kirova Str., Vladikavkaz 362040, Russia, mirag.8184@yandex.ru, ORCID: 0000-0002-9021-7531

Abstract

The paper is focused at the issues of e-democracy in Russia as an innovative form of democracy regarded from the constitutional dimension. The effects of IT penetration to change the appearance, content and methods of legal impact on the environment subject to change are discussed. Due to peculiarities unique to constitutional law and its exceptional role as the legal system backbone, digitization has a special effect on this form of regulation. The evidence in favour of the joint competence of the federal and regional authorities over the issues of information and IT technologies based on constitutional realities is presented. It is argued that e-democracy viewed from the constitutional dimension is above all subject to constitutional regulation. As an instrument of democratic rule politically based on the constitutional imperative of overall empowerment of the people, e-democracy is legitimately part and parcel of constitutional law relying on the relationships between democracy and popular sovereignty. Moreover, popular sovereignty, like other types of sovereignty such as the national sovereignty, is an extension of personal sovereignty as a set of inherent, inalienable human and civil rights and liberties safeguarded by the state. The rights including their digital expression make up a traditional and meaningful subject of constitutional regulation. These are primarily the rights to be exercised in whole or for the most part in terms of digital indicators defining the digital status of each person as predated by the constitutional principle of equality that means digital equality of access to IT technologies for all. These rights primarily embrace the constitutional right to information which is guaranteed to all and which includes the freedom to search for, receive, transmit, produce and disseminate information in any legitimate way (part 4 Article 29 of the Constitution of the Russian Federation). Along with constitutional law, e-democracy is subject to information law as a set of provisions governing social relationships in the sphere of information. It is stated that information law is based on constitutional premises characterizing the principles of Russia's constitutional system.

Keywords
informatization, digitization, law, constitutional law, information law, electronic democracy.

For citation: Lolaeva A.S. (2022) E-Democracy: A Constitutional Dimension. *Legal Issues in the Digital Age,* vol.3, no. 4, pp. 88–105. DOI:10.17323/2713-2749.2022.4.88.105

Background

The 21th century marks a large-scale penetration of publicly available ITC technologies which shape the digital society based on the interactive relationships between society, government and individuals. ITC technologies have crossed the national borders to become part and parcel of the vital functions of society.

Daniel Bell, US. sociologist, wrote in this regard: "The emergence of a new social order based on telecommunications will have a decisive importance for both economic and social life, knowledge generating methods and the nature of human labour in the coming century. The revolution in the organization and processing of information and knowledge where computers assume the pivotal role is unfolding along with the establishment of postindustrial society" [Bell D., 1988: 330].

Of the global trends characteristic of the modern historic period, researchers point at the emerging transition from the hierarchic principle of social (including public authority) relationships to the network principle and networking structures [Mamut L.S., 2005: 11].

Under the Okinawa Charter on the Global Information Society (2000), ITC technologies are a major factor which shapes the society of the 21th century. Their revolutionary impact changes people's way of life, education and work as well as the interactions between the government and civil society[1].

The 2017–2030 Information Society Development Strategy for the Russian Federation approved by Presidential Decree No. 202 of 09 May 2017 qualifies the information society as the one where information and the extent of its availability and use radically affect the social, economic and cul-

[1] Diplomaticheskiy vestnik. Moscow, 2000, no. 8, pp. 51–56.

tural conditions of life[2]. As the jurisprudence points out, the rapid growth of information, emergence of colossal data arrays and databases, intensive development and large-scale penetration of digital technologies into different spheres of social life with expansion into an ever growing number of domains and types of social interaction, activities of public and social institutions is a major development factor of modern society shaping a new "digital" reality [Khabrieva T.Ya., Chernogor N.N., 2019: 85].

Digitization permeates all aspects of social life including law which, being a universal regulator, cannot escape the effects of new digital processes penetrating the legal fabric and changing the appearance, content and methods of legal impact on the environment subject to change. Digital electronic technologies change the world around us and set new objectives to the authorities, society, individuals and their associations.

Basic Part

The digitization of law has a twofold impact on legal development. On the one hand, law becomes instrumental for digitization of the social environment as regards its economic, political, social, cultural, spiritual and other components by establishing legal standards for the use of digital technologies in support of legal regulation of information processes.

Informatization of law thus pursues the purpose of supporting the process of creating technological conditions for an optimal satisfaction of information needs in the areas of governance through efficient use of information resources based on innovative technologies.

Moreover, the legal impact has a global, overarching nature to penetrate and transform the whole range of social links subject to digitization. Law shapes the information infrastructure of society as a set of information objects, systems, sites and networks located within the national territory.

The 2017–2030 Information Society Development Strategy for Russia makes for the need to improve the regulation in respect of safe processing of information (including search, accumulation, analysis, use, preservation and dissemination) and application of new technologies in line with the

[2] On the 2017-2030 Information Society Development Strategy for Russia: Presidential Decree No. 203 of 09 May 2017. Available at: URL: http://publication.pravo.gov.ru/Document/View/0001201705100002 (accessed: 12. 09. 2022)

level of technological development and public interests; ensure a balance between the timely introduction of new data processing technologies and the protection of individual rights including the right to personal and family privacy.

An extensive ITC penetration of socioeconomic sectors and public agencies has enabled an e-government to be established in Russia as an innovative form of governance, with widely used IT technologies ensuring of a new standard of speed and convenience of access to both public services and information on how well the public authorities perform.

On the other hand, law is subject to informatization feedback, only to affect the content, system, structure and forms of law enshrined in the provisions which legalize the social environment in its digital projection and blur the lines between private and public law thanks to the universal instrumentality. According to V.D. Zorkin, new law, "that of the second modernism, is emerging today as a regulator of economic, political and social relationships in the digital world of big data, robotics and artificial intelligence"[3].

The digitization of law has resulted in crystallization of information law as a branch of the legal system focused on digital relationships incorporating the tools for digital interactions between social entities.

Moreover, both of the said processes are simultaneous, parallel, interrelated and essentially inseparable. Law cannot adequately regulate information processes unless it has the provisions characterizing modern telecom technologies adapted to the needs of network communications.

The digitization of law gives rise to new things subject to legal impact such as the digital information environment, data system, ITC network etc.

The digitization changes the range of entities with a legal capacity by adding new parties to digital relationships such as data owners, data system operators, website owners, hosting providers etc.

Legalization is pending for robots as parties to the information environment pretending to have a legal status [Gadzhiev G.A., Voinikanis E.A., 2018:

[3] Zorkin V.D. Law in the digital world: considerations on the margins of Saint-Petersburg International Legal Forum // Rossiyskaya gazeta. 2018. No. 7578. Available at: URL: https://rg.ru/2018/05/29/zorkin-zadachagosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (accessed: 12.09.2022)

24–28]. As observed by some authors, the regulatory environment reveals the relationships "with a new digital entity — robot — to become, if not a legal personality, at least a party" [Khabrieva T.Ya., Chernogor N.N., 2019: 94].

According to E.V. Talapina, individuals as legal parties will establish virtual relationships via the Internet which do not always mimic the real ones. Virtual life has predictable and known from practice legal implications — or doesn't have any. In the virtual space, individuals often hide behind the so-called virtual personality or digital image, with pseudonyms (nicknames) disguising the real person. She writes: "It turns out that personal identification in the Internet is a multi-faceted problem likely to be related to various violations of the rights of a wide range of entities. It can be handled differently. One of the proposed options is to put up with the impossibility to identify a party in the Internet: technical means of identification can create a legal fiction or presume a person but cannot definitely identify a party to legal relationships" [Talapina E.V., 2018: 6–7].

Digital technologies will certainly complicate the identification of parties to legal relationships which is nonetheless mandatory and personalized. The issue can only be about the improvement of identification arrangements as a set of steps to establish and verify personal details. The legal identification of a party based on information contained in the memory matrix of legal provisions is always possible. Once a party is not identifiable in the Internet, it simply does not exist in the legal sense because law cannot be based on legal fictions or presumptions of a person, otherwise it will lose the regulatory power.

Digitization has an impact on the content and amount of rights to trigger the emergence of new provisions and institutions. Thus, under Federal Law No. 187-FZ of 2 July 2013 "On Amending Specific Regulations of the Russian Federation on the Protection of Intellectual Property Rights in ITC networks", the Civil Code of Russia (Chapter 6, Part 1) came to include provisions to introduce the category of digital rights to civil law.

While the Civil Code of Russia has a new section on computer information crime, that is Chapter 28, informatization aspects have required the Code of Administrative Offense, Chapter 13 to provide for an administrative liability for offenses in the area of communications and information.

A special impact of digitization on constitutional law is due to the unique nature of its effects and exclusive role as the legal system's integrator. Ac-

cording to A.A. Tedeev, the new ICT technologies exert an especially powerful influence on constitutional relationships [Tedeev A.A., 2016: 124].

Constitutional law finds in the information environment its own objects of impact to match its subject of regulating the political component of the governance relationships. Thus, constitutional law has come to regulate the digital political environment as an area of interactions between public authorities and the people.

As observed by N.S. Bondar, constitutional law has a special regulatory role to play — and the Constitutional Court to resolve essentially new controversies and conflicts in the digital information sphere — due to the very nature of the relevant relationships that are extremely complex and complicated as they combine public and private principles and affect the basic values of society and state, human and civil rights and liberties [Bondar N.S., 2019: 25–28].

As the law in general, constitutional law is related to informatization in two ways: on the one hand, it is embedding information processes into constitutional law and filling the information environment with constitutional provisions while, on the other hand, it is digitizing constitutional law as a branch and using digital components in the constitutional regulatory mechanisms.

The importance of constitutional law is noticeably growing with intensive digitization of the public sphere regulated primarily by constitutional law, and with progressive transition of political and legal phenomena to the digital dimension, new technological paradigm of digital communications and networking principle of governance relationships.

Digitization of constitutional relationships affects the state of constitutional studies designed to provide a theoretical insight into new constitutional realities in accordance with their purpose, objectives and methodologies. In this regard, S.A. Avakian points to need to identify the objectives of these studies and constitutional law in the context of digital technologies. "In this context, law as a whole and constitutional law should re-invent themselves in the new technological environment and the emerging relationships between people, between individuals and public authorities" [Avakian S.A., 2019: 23].

Digitization is affecting a set of definitions used in constitutional studies, with their vocabulary coming to incorporate the concepts such as elec-

tronic/digital democracy which is synonymic with cyberdemocracy, cloud democracy, network democracy and web democracy, only to require adequate scientific interpretation.

The digitization processes become constitutionally acknowledged to expand the set of categories of the principal law. According to V.D. Zorkin, "digitization processes should be regulated by the Constitution of Russia as having the highest legal effect in the national legal system" [Zorkin V.D., 2018: 1].

A large-scale digitization of public relations has been reflected in the latest version of the Constitution (as amended on 14 March 2020) to include concepts such as "information technologies" and "digital data transaction" (para "j", "m", Article 71) that reflects the realities of the modern information environment.

The President of Russian Federation was the first to suggest adding to the Constitution a provision on the responsibility of the state for cyber security of individuals. At a meeting of the working group for draft amendments to the Constitutions he said that "this need has arisen because such regulation was virtually non-existent before while the development of information technologies is fraught with problems to be addressed". The President asked what and how the state could use to develop the economy through digital technologies, what personal data the state could disclose, to what extent these data could be made public in the information environment and with what implications for the individual involved. "This need in technological development — and big data cannot do without personal data — is paralleled, on the other hand, with the need to ensure personal security"[4].

The "digital" constitutional vocabulary gives birth to a "digital constitution" as the expression of the digital information potential of the principal law positing constitutional institutions in their digital design. In this case, digital human and civil rights, e-voting, e-referendum, e-parliament, e-government, e-justice and e-municipality originating from the relevant constitutional provisions become such institutions of the digital constitution. For example, the constitutional status of the Federal Government cannot be adequately represented without its digital image in the e-government format.

[4] Putin has ordered to implement digital transformation of Russia as fast as possible. Available at: https://www.cnews.ru/news/top/2020-12-04_putin_rasporyadilsya_v_kratchajshie (accessed: 12.09.2022)

While not all constitutional provisions have a digital dimension, this does not prevent the objectification of the digital constitution and also of the *economic constitution* incorporating specifically economic constitutional provisions only. Far from absorbing the entire range of digital relationships, the digital constitution shapes their regulatory focus by establishing the principles of information law. As was observed by S.M. Shakhray, the "digital constitution" could and should become a launching pad, *matrix* for the emergence of digital society rights as it is capable of providing the necessary brickwork for agreement, creative impetus and effective mechanisms for the establishment of a new social order in a new reality of cyber space. This does not mean the development of a parallel constitution written in a programming language or a digital phenomenon created through the use of modern computer technologies. It is about the principal law of information society whose qualities will change all basic institutions of the governance system as well as of constitutional law. "In this case, the word combination *digital constitution* should be understood as a new and unique phenomenon of law" [Shakhray S.M., 2018: 1076].

In its current wording, the Constitution refers ITC technologies, security of persons, society and state in the use of these technologies, as well as digital data transactions to the competence of the Russian Federation (para "j" and "m", Article 71), that is, exclusively to the federal competence, something which does not quite match the reality of the vertical distribution of powers. In practice, the constituent territories engage in both legislative and enforcement activities related to IT technologies. They are quite independent in handling multiple issues related to the development and support of regional data systems and the access to regional information resources governed by regional law. Thus, the constituent territories of the Russian Federation will independently develop IT technologies, something that the federal legislator has never objected against.

In view of the above, it necessary to refer the issues of data and IT technologies covered by the Constitution to the joint competence sphere of the Russian Federation and its constituent territories.

Because of the role and importance of informatization for the exercise of constitutional processes, organization of governance, development of democratic institutions of law in Russia, it is fair to speak about the information basis of the Russian constitutional system as a set of provisions which, along with the political, socio-economic and ideological framework, is a

representation of the information nature of the Russian society and state, constitutional value of information and personal digital status.

In its constitutional dimension, e-democracy is subject, first and foremost, to constitutional regulation. As instrumental expression of democracy as a political process based on the constitutional imperative of popular rule (part 1, Article 3 of the Constitution), e-democracy makes up a legitimate subject of constitutional law based on the relationships between democracy and government by the people. As Ya. V. Antonov points out, electronic democracy like e-voting originates from the constitutional ideas of popular rule and election — in particular, from the idea of popular rule directly exercised by the people [Antonov Ya. V., 2016: 117–125].

Since all other legal relationships grow from those of popular rule, the role of constitutional law is to be the leading, basic branch supporting the legal system as a whole.

It should however be borne in mind that popular sovereignty like other types of sovereignty — national, state etc. — is based on personal sovereignty as a set of inherent, inalienable human and civil rights and liberties safeguarded by the state. The rights, including their digital expression, make up a traditional and meaningful object of constitutional regulation. They assume above all the rights exercised in whole or for the most part in terms of digital indicators defining the digital status of each person as predated by the constitutional principle of equality which means digital equality of access to IT technologies for all.

These rights assume, first and foremost, the universal constitutional right to information which includes the freedom to search for, obtain, transmit, produce and disseminate information in any legitimate way (part 4, Article 29 of the Constitution of the Russian Federation). The right to information means that public and local government agencies and their officers have a constitutional obligation to give everyone an opportunity to review the documents and other materials directly related to his or her rights and liberties (part 2, Article 24).

The constitutional right to information is followed by the constitutional right to reliable information on the environmental situation (Article 42).

The right to information is related to the constitutional freedom of thought and speech (part 1, Article 29) which historically makes it meaningful [Travnikov N.O., 2016: 46].

The rights to digital information include the right to participate in affairs of the state both directly and by delegation (part 1, Article 32, Russian Constitution) whose implementation assumes an open and transparent government, opportunity for free access to information on the activities of government agencies and their officials.

The principle of transparent government is enshrined, in particular, in part 2, Article 100 of the Constitution which provides for open meetings of the Russian Parliament.

Direct participation in affairs of the state is embodied in the digital resource "Russian public initiative" as an expression of web democracy that assumes voting for public proposals to be submitted by individuals as approved by the Presidential Decree "On the Guidelines for Improvement of the Governance System" of 7 May 2012[5].

The rights to information also include the right to refer in person or submit individual/collective petitions to public authorities and local governments (Article 33, Russian Constitution) including in the electronic form. Under Federal Law No. 59-FZ of 02.05.2006 "On the Procedure for Processing Petitions in the Russian Federation", petitions can be filed with any public authority (local government) or official as an e-document.

The constitutional rights also include the right to elect and be elected to a public (local government) office as well as the right to participate in a referendum (part 2, Article 32 of the Russian Constitution) are increasingly exercised by way of e-voting. A reflection of this trend is Federal Law No. 67-FZ of 12 June 2002 "On the Principal Guarantees of the Right to Elect and Participate in Referendum" as amended on 14 March 2022[6] which provides for optional e-voting at elections and referendums where the relevant election/referendum commission may elect to hold remote e-voting (Article 64.1). This principle was used in the mechanism of all-Russia voting to approve the amendments to the Constitution on 1 July 2020 which envisaged e-voting as a form of referendum.

Today the exercise of all constitutional rights and liberties (not only related to information) envisages the use of e-procedures whose scope is ever

[5] Collected Laws of Russia. 2012. No. 19. Art. 2338.

[6] Federal Law No. 67-FZ of 12 June 2002 (as amended on 14.03.2022) "On the Principal Guarantees of the Right to Elect and Participate in Referendum". Ibid. 2002. No. 24. Art. 2253.

extending. Thus, the constitutional right to association is exercised inclusively by way of web associations. The right to privacy of correspondence, telephone communications, postal, telegraphic and other electronically transmitted messages is guaranteed in full in the territory of the Russian Federation under Article 63 of the Federal Law "On Communications".

The constitutional law elements of e-democracy also include the relations of national sovereignty enshrined in Article 4 of the Russian Federation Constitution, reflected in digital (information) sovereignty as the country's sovereign right to regulation of the information space. Under the 2017-2030 Information Society Development Strategy, Russia should promote its sovereign right to determine the information, technological and economic policies in the national segment of the Internet at the international level. According to W. Gong, Chinese researcher, a country's digital sovereignty means independence of the national authorities to pursue information policies and support the information and communication order within the national borders [Gong W., 2005:119].

The national sovereignty is related to the constitutional category of national territory as the physical limit of its extension which in digital relationships comes to be characterized as the information space of ex-territorial nature.

Over the recent years, constitutional studies have been enriched with newly coined terms such as digital constitutionalism, digital constitution and even digital constitutional law as an innovative branch brought forward by digitization of the realities of state and law. As noted by I.A. Kravets, the future may be faced with a legitimate question on whether digital constitutional law is a standalone regulatory branch [Kravets I.A., 2020: 93].

There is no such subject in the content of digital constitutional law in its doctrinal interpretation. Digital technologies used in constitutional processes will not by themselves create constitutional provisions in the physical sense but only support their implementation by electronic communication means. Constitutional law and digital constitutional law are indistinguishable in terms of their subject. While their scope covers an identical range of social relationships, they differ in methods of regulation in such a way that constitutional law determines the general composition of the relationships in their static form whereas digital constitutional law will express their dynamic state by supporting their implementation in digital procedures.

Digital constitutional law exists only in procedural terms as a branch of procedural law identifiable in comparison and in connection with substantive law. As was observed by O.E. Kutafin, "the role of procedural provisions is to determine the order and procedure for the implementation of provisions which enshrine the rights and duties of the parties to legal relationships" [Kutafin O.E., 2015: 95]. In the system of constitutional law, one should distinguish the substantive and procedural provisions as those closely related but not identical.

The e-democracy relationships are governed by procedural provisions which implement the constitutional norms of democracy and popular rule. As a branch of law, constitutional procedural law is fairly well established as a ring-fenced and independent right-conferring entity with the legal sources of its own in the form of election law providing for e-voting, electronic civil initiatives etc.

Apart from constitutional law, the e-democracy relationships are regulated by municipal law to form the institution of e-municipality.

E-democracy is also subject to information law as a set of provisions which regulate social relationships in the data sphere in connection with the production, transmission, dissemination, search and receipt of information, use of information technologies and data protection [Popov L.L., Migachev Yu. I., Tikhomirov S.V., 2010: 11].

It is not accidental that constitutional and information laws make up one and the same field under the existing classification of research occupations awardable with academic degrees — 5.1.2 (sciences of state and law) — to cover research areas such as public law regulation of information and IT (digital) technologies, archive-keeping and data protection; legal regulation of the use of IT (digital) technologies in public authority and public governance.

Moreover, information law relies on constitutional premises characteristic of the information principles of the Russian constitutional system. According to legal literature, "there is an evident link between the constitutional and information law regulation of relationships in information society to make both branches interact as they regulate the relationships in the sphere of information" [Abdrakhmanov D.V., 2022: 58].

Apart from information law, the e-democracy relationships are governed by digital law believed to be equal to information law by a majority

of literary sources since information technologies are believed to be equal to digital ones.

This approach is fairly reasonable as in the information era no data resources can be used outside the latest IT technologies. Under Federal Law No. 149-FZ of 27 July 2006 "On Information, IT Technologies and Data Protection" — the main source of information law — state regulation of IT technologies means regulation of the relationships to search, receipt, transmit, produce and disseminate information through the use of IT technologies (informatization). As observed by A.A. Tedeev, the subject to be regulated by information law should be social relationships that emerge in the process of electronic communications taking place in the information environment [Tedeev A.A., 2006: 4].

At the same time, not all information technologies, that is, procedures and methods of searching, accumulating, storing, processing, providing, disseminating information, are implemented in the digital format. Information as messages (data) of whatever form and method of communication and use (informatization) existed long before the emergence of digital technologies which are a legacy of the recent times called postindustrial. It is only then that information law has absorbed the digital content to include the provisions governing digital technologies as such in connection with electronic data transactions which assume the language of binary calculations. The digital terminology became established in legal studies and law much later than the information terminology.

Like any set of data, information can be not only electronic but also textual, graphical, sonic, visual, harmonic etc., that is, contained in a format which does not require any digital (IT) technologies.

Digital technologies are only part of information technologies that embrace all technologies related to data transactions implementable even through the use of analogue devices. Informatization subsumes digitization but is not limited to it. Digitization is the technological framework of informatization in its current form, a process of making information digital. As observed in the studies of information law, such feature of informatization as the technical and technological principles of satisfying information needs in the legal sphere is very important for understanding the essence of informatization in law. These principles assume a set of actions to design and effectively apply user-friendly data systems for an automated process

of satisfying the information interests in law through the use of computers, digital telephony/telecommunications and high-performance IT technologies [Kuznetsova P. Yu., 2012: 279–280].

Digital provisions as part of information law have emerged gradually as the information environment was digitized and digital technologies replaced analogue ones to form an institution which, on the one hand, is a standalone structural unit of information law covering normatively homogenous, intrinsically arranged legal material, and, on the other hand, a primary element of a new branch of law which provides for comprehensive, relatively complete regulation of innovative digital relationships within a separate segment of law. According to S.S. Alexeev, the young main branch is formed by the gradual transformation of entities typically in the following order: law — legal institution — sub-branch — complex specialized branch — main specialized branch [Alexeev S.S., 1975: 226–227].

The emergence of social processes that required a digital form and special regulation was a physical prerequisite for making digital law an institution in its own right.

As digital relationships spread out to become more specific, the institution of digital law was transformed first into a sub-branch of information law and later into an independent branch which did not coincide with information law in terms of its subject. The subject of digital law is the whole set of digital (digitized) relationships, not only those of information. The system of digital relationships covers those not directly related to information transactions, such as e-services to be provided as part of e-government in support of the public service function though these relationships carry an information component in the form of data they use.

Viewed in terms of its subject matter, functional and structural parameters, digital law can be regarded as a standalone, independent branch of law which has sprung from information law. New branches of law will always stem from those already established as their logical extension.

This branch of law has emerged in response to an objective need to digitize social relationships which require special regulation, and due to the emergence of computer and telecommunication technologies beyond the regulatory scope of the main, field-specific branches of law.

Digital law has all the acknowledged features of a branch of law, the first and foremost being the presence of a particular subject of regulation. As

observed by S.S. Alexeev, the subject of regulation has a primary, systemic importance for branches of law. The subject provides for an objective need in separate regulation of the relationships in question and constitutes the decisive systemic basis just because a known group of relationships and long-felt necessities of social life — whatever is covered by it — objectively need to be specifically regulated through a specific regulatory regime [Alexeev S.S., 1975: 169].

There is every reason to believe that digital law has a specific subject of regulation of its own as a related set of qualitatively homogenous and objectively determined social relationships which make up its identity.

The subject of digital law is made of social relationships which emerge in the process of digitization of law through the use of digital technologies in legal processes as a set of methods to apply computing equipment to accumulate, store, process, transmit and use the relevant information and which comprise electronic resources needed to manage information processes.

Digital relationships as the subject of regulation also predetermine the name of the branch (digital law).

It is not about standards of technical and operational nature which are used, in particular, in programming and which include dedicated software to be used in election processes to generate the keys for encryption and decryption of election outcomes.

Provisions of digital law are durable legal standards regulating the content of digital transactions. As applied to election, these standards define the procedures for anonymization to prevent the use of special software and other arrangements to connect recordable voting results to personal data of voters, and the procedures for authentication to check whether voters really possess the identifiers they use and to confirm their validity.

The institution of digital law is made of digital rights created in the legal information environment which open up the access to digital resources for network communication between individuals and the state. As noted by V.D. Zorkin, digital personal rights are universal human rights which become specific in the digital and virtual space both at the legislative level and at the level they are exercised [Zorkin V.D., 2018].

Digital rights are recognized by legislation as valuable rights to constitute obligational and other rights defined by law as digital whose content

and terms of exercise are determined under the rules of a qualified data system. To exercise and dispose of digital rights including to pledge, transfer and otherwise encumber such rights or restrict their disposal is only possible in the data system without recourse to a third party (Article 141.1, Civil Code of Russia).

Digital rights also include the right of access to the Internet, right of access to telecommunication networks, right to protection of digital personal information, right to protection of reputation of personal identity, consumer's right to protection of privacy including in personal data processing, etc.

Conclusion

The extent of IT penetration into the political and legal environment which transforms the legal position of individuals allows to treat information (and digital) rights as the latest generation of individual rights and liberties characteristic of the personal legal status in the postindustrial society.

E-democracy is regulated simultaneously within several branches of law to form a complex legal institution. At the same time, e-democracy as an institution relies on provisions of constitutional law which enshrines its main legal characteristics and conceptual principles. It is provisions of constitutional law in their primary form that define the institutional system of e-democracy in terms of composition of its parties, its information component, legal format of its implementation, and the extent of its impact on public authorities.

References

1. Abdrakhmanov D.B. (2022) Constitutional principles of informatization of society in the Russian Federation. Candidate of Juridical Sciences Thesis. Cheliabinsk, 244 p. (in Russ.)

2. Alexeev S.S. (1975) *The structure of Soviet law.* Moscow: Juridicheka-ya literature, 260 p. (in Russ.)

3. Alexeeva M.V. (2012) The exercise of the constitutional right for information as one of basic human rights. *Konstitcionnoye i minitcipalnoe pravo*=Constitutional and Municipal Law, no. 7, pp. 16–20 (in Russ.)

4. Antonov Ya. V. (2016) Constitutional principles of e-democracy in Russia. *Sbornik trudov Severo-Zapadnogo Instituta upravlenia*=Collected Papers of the North-West Institute of Governance, no. 1, pp. 117–125 (in Russ.)

5. Avakian S.A. (2019) The information space of knowledge, digital world and constitutional law. *Konstitutcionnoye i munitsipalnoe pravo*=Constitutional and Municipal Law, no. 7, pp. 23–28 (in Russ.)

6. Bell D. (1988) The social framework of the information society. In: A new technocratic wave in the West. Moscow: Progress, pp. 330–342 (in Russ.)

7. Bondar N.S. (2019) The digital information space as a new focus of constitutional law: doctrinal principles and practice. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 11, pp. 25–28 (in Russ.)

8. Gadzhiev G.A., Voinikanis E.A. (2018) Can a robot be a person at law (search for legal forms for regulating digital economy). *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, no. 4, pp. 24–28 (in Russ.)

9. Goncharov I.V. (2019) Constitutional values in the era of "digital technologies". *Konstitutcionnoye i munitcipalnoe pravo*=Constitutional and Municipal Law, no. 11, pp. 15–17 (in Russ.)

10. Gong W. (2005) Information sovereignty reviewed. *Intercultural Communication Studies*, no. 1, pp. 119–135.

11. Information technologies in legal practice (2012) P.Yu. Kuznetsova (ed.). Moscow: Norma, 422 p. (in Russ.)

12 .Khabrieva T.Ya., Chernogor N.N. (2019) State and law in the modern world: issues of theory and history. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 1, pp. 85–102.

13. A.N.Kokotov, M.I. Kukushkin et al. (2010) Constitutional law in Russia: textbook. Moscow: Prospekt, 543 p. (in Russ.)

14 .Kravets I.A. (2020) The digital constitutionalism and the future of information society. *Gosudarstvo i pravo*=State and Law, no. 4, pp. 85–104 (in Russ.)

15 .Kutafin O.E. (2015) The subject of constitutional law. Moscow: Norma, 448 p. (in Russ.)

16. Mamut L.S. (2005) A network state? *Gosudarstvo i pravo*=State and Law, no. 11, pp. 5–12 (in Russ.)

17. Popov L.L., Migachev Yu. I., Tikhomirov S.V. (2010) The information law. Moscow: Yurait, 495 p. (in Russ.)

18. Shakhray S.M. (2018) Digital constitution: the main personal rights in a totally information society. *Bulletin RAN*=Vestnik RAN, no. 12, pp. 1075–1082 (in Russ.)

19. Talapina E.B. (2018) Law and digitization: new challenges and prospects. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 2, pp. 5–17 (in Russ.)

20. Tedeev A.A. (2006) The subject of information law in the Internet context. *Informatcinnoye pravo*=Information Law, no. 3, pp. 3–6 (in Russ.)

21. Tedeev A.A. (2016) Transforming legal system in the IT development context. *Trudy po intellektuaknoy sobstvennosti*=Works on Intellectual Property, vol. 24, no. 1, pp. 123–140 (in Russ.)

22. Travnikov N.O. (2016) Main stages of personal development in the information sphere. *Sovremennoye pravo*=Modern Law, no. 2, pp. 43–46 (in Russ.)

23. Zorkin V.D. (2018) Law in the digital world: thoughts at the Saint Petersburg international legal forum. *Rossiyskaya gazeta*. 30.05.2018. No. 7578. (in Russ.)

Information about the author:

Lolaeva A.S. — Candidate of Sciences (Law), Associate Professor.

The paper was submitted to the editorial office 01.11.2022; approved after reviewing 17.11.2022; accepted for publication 21.11.2022.

Legal Issues in the Digital Age. 2022. Vol. 3. No. 4.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 4.

Research article
УДК: 340
DOI:10.17323/2713-2749.2022.4.106.129

Digitalisation in Russia: In Search of a Legal Model

Dmitry Aleksandrovich Shevelko

Moscow State Lomonosov University, Russia, 1/13 Leninskie Gory, Moscow 119991, Russia, shevelko@audit.msu.ru, https://orcid.org/0000-0003-1355-067X

Abstract

The article considers issues faced by legal regulation of digitalisation in Russia. The aim of the analysis was to formulate theoretical approaches to the current state of legal regulation of digitalisation in Russia and directions for its improvement. To this end, the authors set the objectives to assess the sufficiency and adequacy of legal regulation in Russia and then compare it with the experience of the UK, Germany, Sweden, and Switzerland. Russia has formulated a national goal for building a digital economy. A national programme of the same name and other policy documents have been adopted in accordance with this goal. However, even before this goal was set, a number of strategic planning documents (a strategy and a doctrine) had been adopted in this area in Russia. Our analysis demonstrates that their provisions have only partly been taken into consideration in drafting the new regulation. Actually, in the year 2017 there was one set of goals, and the year 2018 saw a different set of goals. The survey found shortcomings in the legal regulation of long-term digitalisation goals, such as poorly defined contents of the measures, a lack of measurable and concrete actions to develop legal regulations, and a failure to elaborate the structure of the documents. The foreign countries under review have developed approaches to drafting clear and understandable digitalisation strategies. They typically analyse existing entry points, make an inventory of activities in all areas, and identify measurable regulatory initiatives. It would be advisable to apply such approaches in Russia. Of further note are gaps in regulation of government information systems ('GIS') in strategic planning documents related to establishing the cost of GIS development, information availability, and assessment of GIS efficiency. Based on the survey outcomes, the authors suggest that there is a need for a unified digitalisation strategy and better legal regulation in Russia. Due to the shortcomings mentioned in digitalisation, Russia can fail to attain the digitalisation aims and objectives, and begin to lag behind the rest of the world.

Keywords

digitalisation, GIS, information systems, digital economy, legal regulation, digitalisation strategy, expense type.

For citation: Shevelko D.A. (2022) Digitalisation in Russia: In Search of a Legal Model. *Legal Issues in the Digital Age,* vol. 3., no. 4, pp. 106–129. DOI:10.17323/2713-2749.2022.4.106.129

Introduction

Russian public administration and economy have been quickly digitalising in the past five years. Currently, legal matters of preparing federal budget and fulfilling strategic planning documents are under transformation. Most budget processes are in essence performed by means of government information systems ('GIS').

It is possible to identify a number of GIS types used to digitalise budgetary arrangements: integrated government information system for public finance management 'Electronic Budget' ('Electronic Budget'), unified procurement information system for public procurement ('UIS'), Automated Federal Treasury System ('AFTS') for treasury budget compliance, and national project management subsystem for national projects.

There are just a few largest GISs that have enabled transforming budgetary arrangements in the public sector. As this process is now complete, legal GIS regulation has to be analysed and ways to improve it considered.

According to the Audit Chamber of Russia, 67 federal government authorities and public non-budgetary funds control 1143 information systems[1] with an estimated total cost of ownership amounting to RUB 296 billion[2]. Furthermore, there is a large number of information systems at the ministry level, not to mention the regional and municipal levels.

[1] As at 04 December 2022. Report on the results of the conference 'Assessment of the Current Status of Federal State Information Systems in Terms of the Outlooks of Digitalization of Public Administration'. Approved by the Collegium of the Accounts Chamber of the Russian Federation on 28 June 2022. Available at: URL: https://ach.gov.ru/statements/bulletin-sp-8-2022 (accessed: 20.11. 2022)

[2] Ibid.

It is clear from the above figures that the GIS sphere plays a vital role in Russia's development, hence the legislator has to establish an effective legal regulation system. Otherwise, such a multitude of GISs can result in a chaos and gaps in legal regulation.

As at 21 November, 2022, over 175 legal regulations of various levels, including 17 federal laws (10), and over 160 statutory instruments regulate the sphere of GIS and digitalisation at the moment.

The amount of the instruments has grown by 15% over the past two years[3]. They can be grouped into the instruments that directly regulate digitalisation and information management (ca. 50 instruments, or 30%), and instruments indirectly regulating certain individual areas of IT-based management (i.e., they are related on the basis of definitions and particular legal aspects).

Several types of regulatory instruments concerning digitalisation can be distinguished. One of them is instruments determining the target-setting principles for development of that sphere. Two, are instruments related to the funding of the respective measures. Three, are instruments describing requirements to the GIS.

While the GIS sector is only one of digitalisation areas, it is the most important one as it underlies the functioning of the government, certain public sectors (education, health care etc.) and interaction with the people and the private sector. Other spheres include implementation of private projects, where the government has been working to ensure the best legal environment and favourable economic conditions.

The large numbers of information systems and legal acts also calls for a proper setting of top-level goals: Where digitalisation is going, and what the state, business and the public should get.

Digital Transformation is one of the national goals that the President of the Russian Federation has set forth in the programme for long-term development until 2030[4]. The four target indicators to control progress towards this goal are: achieving digital maturity; increase in the share of services provided in the public interest; broadband internet access; increase in investments in Russian-made solutions.

[3] From 20 December 2021 to 21 November 2022.

[4] Sub-paragraph "д", Para 1 of Presidential Decree No. 474 of 21 July 2020 'On National Development Goals of the Russian Federation for the period until 2030' // SPS Consultant Plus.

The Digital Economy national programme, Russian state-run programmes and federal projects have been adopted to ensure this national goal is achieved. The main focus in these documents is on measures to develop public administration and economy, but planning and implementation of the optimum legal model for supporting the digitalisation of Russia also play an important role.

We believe that the current state of affairs in digitalisation, including digitalisation in the government sector, calls for expert analysis and rethinking, including a comparison[5] between legal methods applied in various countries to develop the legal environment and ensure the best result.

The aim of research is to formulate theoretical approaches to the current state of legal regulation of digitalisation in Russia and directions for its improvement. S

The author set the following tasks:

Analyse international experience in digitalisation, including approaches to target-setting and systems of legal regulation;

Determine whether the long-term goals of Russia's digitalisation are adequate;

Analyse the measures for establishment of an optimal legal model for digitalisation;

Review the current legal framework and the challenges of digitalisation of the public sector.

The author methods are: comparative legal one, dialectical, legal interpretation and formal legal method. The subject of the study is the legal norms regulating social relations in the field of public sector digitalisation.

1. A Sketch of International Experience of Approaches to Legal Regulation of Digitalisation[6]

It has a sense to preface our study of international experience with a note that adopting a corresponding strategy is the most common legal ap-

[5] As a priority for digitalization.

[6] The section on foreign experience was intended to follow the study of legal regulation in Russia. At the same time, after the drafting of the article, it became evident that the problems of Russia can be better exposed through the analysis of documents from foreign countries.

proach to implementing digitalisation. Such a strategy usually determines a set of key points to be achieved, links goals and objectives, and defines the country's positioning on the international market.

It should be noted that digitalisation of a state leads to competition between countries for digital assets, investments, and for creation of a favourable climate for generating digital products. This competition stems from identical technologies of building IT infrastructure in various countries, which enables choosing between a number of proposals in such countries, while the company will provide its services globally. Of further note is competition for human resources: easy electronic interaction with the government is an advantage that helps attract valuable talents into the economy.

But competition exists not only in the technology aspect. Legal models of regulation also compete against each other, and investors (companies, individuals) prefer the most effective, clear and easy to understand norms and regulations.

At the same time, digitalisation of the public sector remains in the public limelight: It is becoming clear that by digitalising respective processes and services the government grows more effective. Hence, the more automated components there are, the quicker a service is provided, the lower is the risk of an error, and more budgetary funds are saved and can be spent on other projects.

It is impossible to create a digitalisation model without the tools for enforcing this process. In particular, gaps in law, and failed rules must be eliminated, and flexible regulations for a breakthrough in the respective areas created.

As an OECD analysis of 38 countries [Gierten D., Lesher M., 2022: 3] notes, the available legislative framework (e.g., laws on personal data protection or on digital security) should ensure coordination between the digitalisation strategy and specific regulations.

In view of the above, it is still a highly relevant task to study international experience despite the sanctions and challenges in international politics. Situations can change, but, ultimately, countries will continue to compete, and sanctions should not stop the legal development of digitalisation.

This study analysis the current experience of digitalisation in the UK, Federal Republic of Germany, Sweden, and Switzerland. These countries were selected due to the high digitalisation level and quality of legal regulation.

The analysis focused on the existing strategies of digitalisation, measures to enforce its implementation, process descriptions, and measurable and specific end results.

1.1. Germany's Experience in Digitalisation

In June 2021 Germany has adopted the Digitalisation Strategy[7], a long document that offers a concrete solution for every task. While Germany did not set any large-scale digitalisation goals, the document notes that strategic planning implies regular analysis and tracking of progress towards the goals.

The Strategy outlines five tasks: digital literacy, infrastructure and equipment, innovations and digital transformation, society in digital transformation, and the modern state. The Strategy not only develops new activities and directions, but has also structured the extensive work on going since 2016 [Hermann P., 2022: 3].

E.g., steps to create apps for the sick in the health-care sector included analysing the implementation stages since 2019 and assessment of the changes made in law. The results were used to adjust the Strategy's implementation stages.

The Strategy provides for ca. 110 legislative measures to support its implementation. These measures are very clear and easy to understand: e.g., make changes in the Law on Telecommunications to encourage investment in fibre-glass networks and promote joint initiatives of the public and private sector[8]. The measure 'Make Solutions Based on Verifiable Algorithms'[9] provides for continuous monitoring current legal regulation of this issue in Germany, in the European Union and worldwide. The subject of the analysis is regulation of specific risks pertaining to algorithm-based systems.

Documenting the current progress of implementation measures is another important direction of the Strategy.

Digitalisation of the public sphere in Germany implies not only adopting or adjusting regulations but also enforcement, namely: creating digital tools to enforce the provisions of law.

[7] Available at: https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002 (accessed: 25.06.2022)

[8] Ibid. P. 42.

[9] Ibid. P. 164.

E.g., the Law on Online Access[10] has obliged the authorities to be able to provide administrative government services online by the end of 2022. In pursuance of the Law, the federal digitalisation programme[11] was adopted in 2018 that listed 575 services, which were then 'digitalised' from 2018 till 2022.

In conclusion it should be noted that Germany Digitalisation Strategy includes measures for all the digitalisation spheres: the state (e.g., electronic adoption of laws and regulations), health care, education, housing and utilities (online utility calculator), and many other areas.

Therefore, the approach to building the Digitalisation Strategy in Germany involves not only mid-term planning but also documenting the existing achievements and tracks, which generates a comprehensive picture of the digitalisation process. The goals and measures of digitalisation are analysed in terms of their enforceability.

1.2. UK Experience in Digitalisation

The UK Digital Strategy[12], adopted in June 2022, is the current high-level document; the previous version was adopted in 2017. The goal state to be achieved upon its implementation in 2025 is 'a transformed, more effective digital government that delivers better outcomes for all'[13]. Six mission challenges have been set forth for the government:

Civil service transformation that achieves the right results.
One System (One Login) for Government.
Digital improvement for decision making.
Efficient, secure and sustainable technologies.
Developing digital skills.
Unlocking the opportunities of digital transformation.

To implement the Digital Strategy, the UK government has adopted a road map with concrete steps until 2025. It should be noted that the

[10] Available at: https://www.gesetze-im-internet.de/ozg/ (accessed: 16.08.2022)

[11] Available at: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/themen/digitalisierungsprogramm-foederal/foederal-node.html (accessed: 16.08.2022)

[12] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089103/UK_Digital_Strategy_web_accessible.pdf (accessed: 16.08.2022)

[13] Ibid. P. 4.

authors of the road map took into account the recommendations that the National Audit Office[14] made the based on the audit findings in the previous years.

One of the measures to be carried out as part of legal regulation is reforms of the data protection law including raising the data protection standard. In particular, the UK has been improving the Online Safety Bill since 2018[15], which will lay a foundation for a cross-border data flows [Tranos E., Kitsos T., Ortega-Argilés R., 2020: 1929]. As at November 2022, the draft has passed on second reading in the UK House of Commons.

In June 2022 the Queen also announced a legal reform aimed at changing the Data Protection Act and adopting the Competition and Consumer Bills, and the Digital Market Bill[16].

According to the plan, in order to complete the public service mission, uniform standards for service provision will be created and approved. As the regards the single entry point for the government, administration departments will coordinate an overall strategy and roadmap until 2023.

Thus, the analysis suggests that the legal model for digitalisation in the UK includes a limited range of acts (projects). The analysis of the projects shows that they tackle (intend to tackle) the majority of social relations in the sphere of digitalisation.

1.3. Sweden's Experience in Digitalisation

Sweden adopted the Digitalisation Strategy[17] on 20 December 2016 for a period until 2025. The Strategy sets forth the mission to create a sustainable and digital Sweden. The overall strategic goal is 'Sweden will be the world's best country in terms of digital opportunity utilisation'.

The overall goal is broken down into five subgoals: Competence, Security, Innovations, Infrastructure and Governance. E.g., with respect to

[14] The highest audit authority in the UK.

[15] Online Safety Bill. Available at: https://bills.parliament.uk/bills/3137 (accessed: 16.08.2022)

[16] Available at: https://lordslibrary.parliament.uk/digital-regulation/ (accessed: 31.10.2022)

[17] Available at: https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf (accessed: 31.10.2022)

Competence, " In Sweden, everyone should be able to develop and use their digital skills."[18]

Unlike the UK and Germany, Sweden's digitalisation strategy does not include direct measures to develop a legal framework. It sets forth certain simple and straightforward requirements to the regulatory system [Borg, 2018: 40]. Sweden has decided that a modern digital society needs a long-term sustainable legislation that supports development and its potential to improve efficiency.

To achieve the goals of the Strategy, Sweden needs to reform its legislative capacity to create better conditions, and to adjust the laws that unnecessarily complicate digitalisation.

Enforcement measures are set forth in other documents adopted in pursuance of the Digitalisation Strategy. It is worth stressing that, as far as Sweden and Germany are concerned, digitalisation legislation is also developed on the basis of common European Union legislation and directives.

Sweden is an example of non-specific approach to shaping regulatory measures in a strategy. That said, Sweden holds a leading position in the world in terms of legal regulation.

1.4. Switzerland's Experience in Digitalisation

In 2020 the Digital Switzerland Strategy was adopted[19]. According to OECD estimates based on continuous monitoring in 28 countries, Switzerland took the leading position in digitalisation in 2021[20].

The Strategy outlines the principles of digitalisation based on the need for the state, business and citizens to work together to achieve five digitalisation goals. It then lists legal regulation measures required to implement the principles and goals. The list notes which of the provisions should be revised based on the digitalisation goals.

The Digital Switzerland Action Plan, which is part and parcel of the Strategy, defines actors and deadlines.[21] The Action Plan lists 111 activities in all

[18] Ibid. P. 12.

[19] Available at: https://www.digitaldialog.swiss/fr/ (accessed: 24.10.2022)

[20] Available at: https://www.oecd.org/digital/digital-government/ (accessed: 24.10.2022)

[21] Available at: https://www.digitaldialog.swiss/de/aktionsplan-digitale-schweiz-12-2019 (accessed: 11.07.2020)

areas of governance and economy. Based on the analysis results, each activity is detailed, responsible actors assigned, and implementation deadlines set.

Before the list of activities was prepared, the current state of affairs in each respective area had been analysed. E.g., a survey of 5G telecommunications was carried out in 2019 for the target state 'Switzerland has a nationwide, competitive, reliable, efficient and sustainable communications infrastructure.'[22] Thus, the Swiss experience can be used as a best practice in developing digitalisation activities.

Some distinctive features of legal regulation in these countries are clear

One, the set of goals (sub-goals) in the countries analysed are identical. The governments prioritise the areas of human capital, infrastructure, security and the public sector. All the government's position themselves as 'the best' at creating digital tools.

Two, the government's digitalisation strategies have a set of clear and explicit measures for legal regulation, or requirements for such regulation. Legislative initiatives are seen as a precondition for achieving the goals.

Three, the governments perform a mandatory entry point study to commence the implementation of activities and their final evaluation. The results are necessarily reflected in the digitalisation strategy. The final results are subject to internal and external evaluation.

2. Defining Strategic Goals for Digitalisation in Russia

In Russia a solid number of documents define the goals and objectives of digitalisation. We do not have a single digitalisation strategy; the following strategic planning documents contain individual elements. As S.M. Zubarev points out, there are "serious risks of destabilisation of the digitalisation process due to the lack of unity of normative goals, objectives, as well as measures to achieve them." [Zubarev S.M., 2020: 27].

In 2017, the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030[23] (hereinafter–Strategy') was adopt-

[22] Available at: https://www.bafu.admin.ch/bafu/de/home/themen/elektrosmog/dossiers/bericht-arbeitsgruppe-mobilfunk-und-strahlung.html (accessed: 11.07.2020)

[23] Presidential Decree No. 203 of 09 May 2017 on the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 // Corpus of Legislation of the Russian Federation of 15 May 2017. No. 20, p. 2901.

ed, which defines the goal "Create conditions for the formation of a knowledge society in the Russian Federation". Digital economy is defined as a 'national priority.' Initially, the Digital Economy programme was adopted in pursuance of the Strategy. In particular, it is emphasised that the programme "aims to create the conditions for the development of a knowledge society in the Russian Federation."

In 2018, a national objective was adopted: digital transformation. As we will see below, it is not aligned with existing strategic planning documents. Let us have a closer look at them.

The analysis and decomposition of the building blocks of the Strategy have revealed the following:

The Strategy identifies five priorities in the development of the information society. It has a special section for four of the five priorities where it sets a separate priority objective and defines indicative directions for its implementation.

For the priority 'Creating a new technology basis for economic and social development', only 20 main tasks have been identified, without areas for implementation.

Thus, the Strategy is deficient from a legal point of view because it lacks structural coherence and comparability of the objectives, directions, and tasks in its sections. Furthermore, the Strategy lacks the table of contents which complicates understanding of the document for citizens without a legal background.

An analysis of the directions shows that they are not clearly formulated, and the progress towards them cannot be evaluated because there is no timeframe for their implementation and no defined outcome. Let us look at some cases.

The direction outlined for the information space creation priority is "To carry out activities in the field of spiritual and moral education of citizens."[24] It is not clear from the contents of this direction how to implement it.

In respect of stable functioning of the IT infrastructure, the Strategy provides for "centralised monitoring and management of the Russian Fed-

[24] Subparagraph 26(a) of the Strategy.

eration's information infrastructure."[25] As at 21 November 2022, no legal regulation on monitoring was adopted. Also, there were unresolved problems in the management direction. E.g., there is no united approach to assessing the cost of digitalisation at all levels of the public sector system. Evaluation and data collection can be recorded under expenditure type code 242, but there are also borderline codes used to document procurement of equipment and activities related to digitalisation.

A total of 96 implementation directions were defined for four priorities. Only tasks, and not directions, were outlined for one of the priorities. This means that in essence there is no single approach to describing the priorities. The section in question was drafted by different authors without coordination of theirs work. This impairs the quality of legal regulation.

The Strategy provides for only six priority directions for legal regulation. Their analysis shows that, like other activities, they are generic and non-specific. It is not clear from their content what legal regulations can be adopted and what these should contain. As a result, actors may interpret approaches to activity implementation at their own discretion.

The following examples can demonstrate this: "Improve the mechanisms of legislative regulation of the mass media"[26], "Amend the laws of the Russian Federation to ensure that the legal and regulatory framework corresponds to the pace of development of the digital economy."[27]

It is clear: to be able to follow a result, its measurability and quality, it would be useful to include specific measures for the development of digitalisation in strategic planning documents. Otherwise, it appears that when the document was adopted, there was only one task, i.e., to approve it, and that all the directions were to be developed during the implementation period.

Para 53 to 54 of the Strategy state that the timeframe for implementation is defined in the implementation plan. That is, there was an intention to clarify the directions and activities. But, as at 21 November 2022, there was no information on the adoption of such a plan on the Internet or in the legal databases.

---

[25] Subparagraph 29(a) of the Strategy.

[26] Subparagraph 26 'p' of the Strategy.

[27] Subparagraph 42 'ж' of the Strategy.

The implementation plan, as stipulated, was to set forth the legislative support measures for the implementation of the Strategy, namely which legal regulations would be adopted for its implementation.

Therefore, the Strategy is formal: There are legal gaps in defining specific activities and there are no indicators to monitor it. If to compare it with the approaches taken by foreign countries, it would be advisable to consider developing a new unified digitalisation strategy.

Another strategic planning document that can be highlighted as regards digitalisation is the Information Security Doctrine of the Russian Federation, approved by Presidential Decree No. 646[28] (hereinafter — the Doctrine). International experience shows that ensuring information and personal data security is a priority for digitalisation in most of the countries analysed.

In terms of the quality of legal regulation and the decomposition of objectives and activities, one could note the following.

The Doctrine consists of five sections that are not interconnected with each other.

Section 1 lists the terms and definitions used.

Section 2 of the Doctrine formulates the five national priorities in the information sphere. However, they are only listed, and no links are made between the areas of implementation and other elements of the Doctrine. In our opinion, a formal enumeration of certain provisions overburdens a strategic planning document. Such a document defines the areas that the state wants to achieve, so it would be advisable to show directions and activities to achieve specific outcomes for the development of national interests.

Section 3 lists the main information threats and the state of information security. However, the associated risks are only stated, and there are no measures to mitigate them at least to an acceptable level.

The Doctrine does not have a separate objective for the entire document, but Section 4 highlights three strategic objectives for information security in the fields of defence, science and strategic stability.

Section 5 of the Doctrine 'Organisational foundations for ensuring information security' defines the principles and tasks of state security agencies.

[28] Presidential Decree No. 646 of 5 December 2016 'On Approval of the Information Security Doctrine of the Russian Federation' // SPS Consultant Plus.

In addition, there are several more strategic planning documents that make a reference to digitalisation[29]. These are however indirectly related to the documents reviewed, only to the extent that they indicate some aspects of digitalisation.

The National Strategy for the Development of Artificial Intelligence until 2030[30] states the need to create and enforce legal conditions for accessing data and testing solutions based on artificial intelligence.

Clearly, the Doctrine foresees non-public implementation and accountability. However, the two documents reviewed share similar problems and shortcomings with regard to the quality of the legal regulation.

3. Two Digital Economy Programmes

A Digital Economy programme was adopted in 2017 in order to implement the analysed strategic planning documents.[31] And after the approval of the national objective, the national programme 'Digital Economy' ('the national programme') was adopted.

To investigate further, let s examine the two Digital Economy programmes with regard to the quality of legal regulation, and the differences between the two programmes over the two years of their implementation.

There are three major objectives in the Digital Economy programme[32]:

to create an ecosystem for the digital economy of the Russian Federation;

to create the necessary and sufficient institutional and infrastructural conditions;

to increase Russia's competitiveness in this area.

Section 3, 'The Russian Federation in the Global Digital Market', notes that there is a significant lag from the world leaders in the development of the digital economy. One of the reasons appeared to be gaps in the norms

[29] Para 20(a) of the Strategy for Scientific and Technological Development of the Russian Federation, approved by Presidential Decree No. 642 of 01 December 2016: 'The transition to advanced digital technologies, robotic systems, new materials and construction methods, development of big data systems, machine learning and artificial intelligence'

[30] Approved by Presidential Decree No. 490 of 10 October 2019.

[31] Decree of the Government of the Russian Federation No. 1632-p of 28 July 2017.

[32] A high-level summary.

and regulations on digital economy. To overcome it, the Digital Economy programme sets out regulation as a basic direction of the digital economy development.

It is understood as "the creation of a new regulatory environment that ensures a favourable legal regime for the emergence and development of modern technologies, and for economic activities related to their use (the digital economy)".[33].

Six 'indicative' areas of implementation have been identified under this direction. These include, for example, "removal of key legal barriers", "development of comprehensive legislative regulation of relations", and "adoption of measures aimed at encouraging economic activity."

In our opinion, yet another case of unclearly stated implementation directions in the preamble of the Programme may indicate poor project planning. It appears that at the time the Programme was developed and adopted, the responsible authorities had not carried out an inventory of regulation, nor had they identified the risks of legal gaps and shortcomings.

The Digital Economy programme outlines a roadmap with 21 tasks and 56 milestones for the six areas of regulatory implementation. An analysis of the tasks and milestones has shown that different approaches were developed for them: Some do contain specific measurable activities (e.g., "A draft concept of priority measures to improve legal regulation has been prepared"[34]). But most contain very vague actions (e.g., "Regulations have been adopted to create the legal conditions for the creation of a single digital environment of trust"[35]). It is not clear what changes in regulations are required, and what legal mechanisms and instruments will be stipulated in the new rules of law.

The Programme did not immediately identify the responsible actors because the intention was to develop the entire package of areas for legal regulation improvement after the Programme commencement. This raises questions about the ability to monitor the current state of the Programme and the lack of understanding of the final outcome of digitalisation.

[33] Page 10, Section Four 'Digital Economy of the Russian Federation' Programme // SPS Consultant Plus.

[34] Para1.2.1 of the Roadmap

[35] Para 1.7.2 of the Roadmap.

So, there are all the same mistakes in the Programme identified in the Strategy and the Doctrine, despite the fact that a separate drafting and adoption methodology has been selected for the Programme, and strategic planning documents are prepared on the basis of legal requirements[36].

According to the plan, main part of legal regulation was to be carried out in 2018-2020. The adoption of national goals and national projects (programmes) has, however, led to adjustments in objectives and milestones within the new system of strategic planning documents. As a result, the Digital Economy programme was deemed invalid in 2019[37].

The Passport of the National Programme was developed[38] according to methodology[39] different from the previous one. This resulted in structural differences between the two documents: the National Programme has no section on general baseline data, targeting and analysis of entry points. The structure of the Digital Economy National Programme distinguishes federal projects designed for the programme implementation.

The justification documents for the adoption of the Passport may have justified the activities and calculated the risks, but no information about them is available in the public domain.

The Passport of the National Programme distinguishes a separate federal project 'Regulatory framework for the digital environment' as part of the legal regulation[40]. It gives a detail description of the task[41] to ensure enforcement of digitalisation 35[42] of results for achieving it.

---

[36] In accordance with the Federal Law of 28 June 2014 No. 172-FZ 'On Strategic Planning in the Russian Federation' // Corpus of Legislation of the Russian Federation 30 June 2014, No. 26 (Part I), Art. 3378.

[37] Decree of the Government of RF 12 February 2019, No. 195-r // SPS Consultant Plus.

[38] Passport of the National Project 'National Programme 'Digital Economy of the Russian Federation'. Approved by Presidium of Presidential Council for Strategic Development and National Projects, Minutes No. 7 of 4 June 2019.

[39] In accordance with Guidelines for Development of National Projects (Programmes) approved by the Government on 6 June 2018.

[40] Passport of the Federal Project 'Legal Regulation of the Digital Environment' (approved by the Presidium of the Government Commission on Digital Development and the Use of Information Technology to Improve Quality of Life and the Business Environment, Minutes No. 9 of 28.05.2019)

[41] A system of digital economy's legal regulation based on a flexible approach in each area has been established, and civil transactions on the basis of digital technology has been introduced.

[42] As at 21 November 2022.

As at 21 November 2022, half of the results had already been achieved, which is not a bad outcome since research papers note that a comprehensive modernisation is required to regulate digitalisation [Tikhomirov Yu.A. et al., 2021: 8].

It is worth noting that the set of legal tools and results has been partly revised vs. the initial legal objectives set out in the 2017 programme.

Hence, the aims and objectives of digitalisation have been revised in two years. The new paradigm of national objectives does not take into account the provisions of existing strategic planning documents. Therefore, either the documents need to be revised or the planning process needs to be clarified by leaving only the national objectives because the said objectives have not been implemented in the budget legislation nor in the laws on strategic planning documents.

4. Present Day Challenges

There are several long-standing problems in jurisprudence with respect to digitalisation of the state and public sector that have not been resolved to date; some were studied by scholars as far back as 2016 [Amelin R.V., 2016: 10–12].

4.1. GIS Regulation

In the government sector, there are no uniform approaches to the functioning of GISs, software and other products. As indicated, the authorities possess a large array of GISs. The legal grounds for their creation varied: some were created on the basis of mandates, some by the bylaws, and so on.

Basic GIS regulation is moving to the sub-legislative level, which leads to "an expansion of legal regulation not envisaged at the state level" [Zaloilo M.V., 2019: 23]. There is no 'inventory' of the justifications, cost of ownership, or expediency of GIS creation at present. Strategic planning documents do not envisage a solution to this problem.

At the same time, the growth of GIS leads to an 'unmanageable' chaos in legal regulation, because at the legislative level the main regulation of GIS is found in Article 14, Federal Law No. 149-FZ of 27 July 2006 'On Information, Information Technology and Information Protec-

tion'[43]. The legal regulation then descends to the sub-legislative level, where there is no uniform hierarchy of regulations. As part of the Digital Economy national programme, super-services are being created that integrate the existing GIS capabilities of the authorities.

Hence, a question also arises about data integration in the GIS and data input-output. There are no uniform requirements on the respective parameters in the law. The state has to pay a lot of money for adaptation of inputs and outputs.

4.2. Estimating Costs of GIS

If we consider that more sanctions were imposed on Russia in 2022, the task of substituting foreign software is now even more relevant. One of the issues in the legal regulation of GIS is regulating the calculation of the cost of establishing and maintaining a GIS, and treatment of the digitalisation cost within the country. Experts note gaps in law pose a high risk for digitalisation.[44]

By Procedure for the Formation and Application of Codes of the Budget Classification of the Russian Federation, their Structure and Purpose Principles approved by Order of the Ministry of Finance No. 85n[45] of 6 June 2019, budget expenses in the field of information and communication technologies are displayed under Expense Type 242.[46]

Despite the fact that there is only one type of expenditure, there is no open information on the total expenditure for that type of expenditure (e.g., in the Federal Treasury's Automated System). The government may possess this information, but ordinary researchers cannot estimate the costs.

Then there is the borderline type of expenditure, Type 244, that can be used to estimate costs, e.g. for maintenance, or costs close to digitalisation. In view of this, it is probably advisable to clarify the procedure for applying

[43] Federal Law No. 149-FZ of 27 July 2006 'On Information, Information Technologies and Information Protection' // Corpus of Legislation of the Russian Federation 31 July 2006, No. 31 (Part 1), Art. 3448.

[44] Digital Transformation of Industries. Moscow, 2021. P. 173.

[45] Order of the Ministry of Finance 'On the Procedure for the Formation and Application of Codes of the Budget Classification of the Russian Federation, their Structure and Purpose Principles'. Available at: http://pravo.gov.ru (accessed: 12.05.2020)

[46] Starting from 2023, also reflected under this Expense Type due to the new procedure for Budgetary Classification Code application.

Expense Type 244 and establish requirements on transparency of information on government spending on digitalisation.

Regarding Russia as a federal state, regional and municipal budgets are important in estimating the overall costs of digitalisation of the public sector. However, these budgets reflect Expense Type 242 expenses separately in their IT systems. Hence, there is no single reliable statistics on digitalisation expenses all the way down to the municipal level.

4.3. Costs of GIS Creation and Open Source Code

Establishing the cost of GIS creation is the most challenging task in digitalising state-funded activities. At present, most of the costs are reflected in accordance with the rules for determining the initial (maximum) price ('Maximum Starting Price of Contract/MSPC') based on the laws on government procurement.

The key challenge here is to find similar GISs to estimate the costs. To calculate the price, government authorities can receive three commercial offers from any market participant. Since technical data and requirements to GIS are incomparable (including OKVED Russian Classification of Economic Activities Codes and OKPD Russian Classification of Products by Economic Activities Codes for procurement specified in the Unified Information System), analogues cannot be used to estimate the MSPC.

It would be advisable in this respect to develop an open source software code that can be used by several government authorities. E.g., such a direction occurs in the UK Digital Strategy: you pay once, and everyone benefits. However, using a single code calls for the definition of regulatory legal requirements.

At this stage, it would be appropriate to analyse the available GISs, identify their features and functions so as to improve them. Such an exercise could reduce GIS maintenance costs because updating and upgrading the GIS is becoming a pressing issue. Oftentimes, government authorities cite changes in legal regulations to justify the need for more procurement, which calls into question the flexibility of the original GIS functionality.

In our opinion, Russia's digitalisation strategy may include a direction for optimisation of GIS development and maintenance costs, including legal regulation.

4.4. How to Estimate Digitalisation and GIS Efficiency

One more key question in analysing whether the digitalisation aims and objectives have been attained is how to estimate the cost-effectiveness of digitalisation (GIS creation and maintenance). Now the approaches involve assessing the implementation of a national programme or a federal project. They provide for a methodology and a set of indicators. Their analysis shows that they are based on attaining indicators and outcomes. The Russian Audit Chamber also carries out an on going assessment [Savina N.V., Buryakova A.O., 2022: 19], but only as part of the evaluation of federal expenditures.

However, such approaches fail to satisfy the need for long-term assessment of GISs, including questions such as whether a GIS allows services to be provided without changes, how many failures a GIS has had, and whether there were alternative ways to achieve the objectives. Studies at the municipal level also support introduction of a long-term GIS performance assessment [Ulyanov A. Yu., 2022: 45].

There is no GIS project solution assessment centre now directly related to the aforementioned problem of estimating the GIS cost. To get an approval for budget allocations, it is in most cases enough for government authorities to upload a completed plan to the Federal Government Information System for Coordination of Informatisation. We believe that this problem can be solved by creating a national register of digitalisation tasks in Russia that would include data on existing GISs at all levels and on tasks that must be digitalised.

To evaluate the GIS effectiveness, an appropriate methodology must be developed and a detailed analysis on available GISs performed.

4.5. Digitalisation Reporting Data

In course of this survey, it was encountered a trivial issue: difficulty in finding information on the Digital Economy programme, the federal project, and reporting about them. There is a specialised web-site[47], but it does not contain either the original or the latest versions of the programmes. Similarly, passports of strategic planning documents could not be found on

[47] Available at: https:/ national projects.rf/ (accessed: 12.11.2022)

the world-wide web. Overall information in understandable format can be found, but without reference to the respective legal regulation.

E.g., a search for data on the implementation of the Federal Project 'Regulation of the Digital Environment' returns a passport with 17 results on the web-site of the Federal Government. However, current version on web-site of the Ministry of Economic Development[48] contains 35 results.

One more example: web-site of the Federal Government Information System for Coordination of Informatisation[49] contains plans, features public information about them for the latest available years 2019–2021. Clearly, some data in the FGIS for CI may be confidential, but Russian citizens are in their capacity of taxpayers entitled to know about the government's total digitalisation expenses.

There are also problems with reporting on the implementation of the Digital Economy National Programme. Only one report for 2020 may be found on the Internet. This raises debates about providing information for potential users: why it is impossible to use a single source would contain all available information on projects and programmes.

At first, you did not even anticipate unavailability of information on the implementation of strategic planning documents. But, as it is possible to see, digitalisation in Russia faces 'childish' issues of posting information on its progress.

Conclusion

Foreign countries implement single approaches to developing digitalisation strategies. These include the mandatory examination and publication of the target state for the development of measures, formation of a matrix of legal measures for the implementation of the strategy, use of clear and concise language, and use of comparable criteria for the evaluation of the final outcome.

Russia's strategic planning documents in the area of digitalisation have common shortcomings in legal regulation: there are no specific measurable

[48] Available at: URL:https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/?ysclid=larpv09rfv357701744 (accessed: 31.10.2022)

[49] Available at: URL: https://portal.eskigov.ru (accessed:12.11.2022)

activities, no unified structure, and they contain formal elements. We believe that, in view of the above, questions arise on the need for such documents.

Due to outdated digitalisation directions, priorities and goals in strategic planning documents mentioned, Russia needs a separate strategy for digitalisation. The new strategy should link all digitalisation activities and define clear goals and objectives over time.

An analysis of the Russian digitalisation objectives and legal model shows that we are losing out to competition from foreign countries at the current stage. This is not even related to technology solutions that are more difficult to implement due to the sanctions. The reason is lack of harmonisation of the legal framework, and of clear and concise legal norms. At the moment you cannot get a clear answer as to what the government, the public and business would receive from digitalisation.

Legal monitoring strategic planning documents construction, legal decomposition of goals, objectives and measures would be useful. It is critically important to build a system with a uninform approach, from strategies to concrete projects and programmes.

Strategic planning documents now do not contain measures to address digitalisation challenges in the public sector, namely approaches to determining the GIS creation cost and assessing the efficiency of spending on GISs.

Digitalisation in Russia, despite lofty goals, has been facing simple problems of posting information on the latest versions of strategic planning documents and reports on their implementation.

References

1. Amelin R.V. (2016) Legal regime of government information systems: textbook. Moscow: Grosmedia, 103 p. (in Russ.)

2. Amelin R.V. (2017) Regulation of social relations in the sphere of information systems. *Aktualnye voprocy rossiyskogo prava*=Current Issues of Russian Law, no. 12, pp. 68–77. Available at: https://doi.org/10.17803/1994-1471.2017.85.12.068-077 (accessed: 15.01.2021) (in Russ.)

3. Artyukhin R.E., Povetkina N.A. et al. (2021) New institutions of budget law in the digital revolution. Moscow: Norma, 192 p. (in Russ.)

4. Borg M., Olsson T. et al. (2018) Digitalization of Swedish Government Agencies. A Perspective Through the Lens of a Software Development Census. Available at: 10.1145/3183428.3183434 (accessed: 10.04.2022)

5. Digital transformation of industries: starting conditions and priorities (2021) Reports to the 22nd April International Conference on Economic and Social Development. Moscow: HSE Publishing House, 239 p. (in Russ.)

6. Digital transformation of public administration: myths and reality (2019). Reports to 20th April International Conference on Economic and Social Development. Moscow: HSE Publishing House, 43 p. (in Russ.)

7. Gierten D., Lesher M. (2022) Assessing national digital strategies and their governance. OECD Digital Economy Papers No. 324. Available at: https://doi.org/10.1787/baffceca-en. (accessed: 20.11.2022)

8. Hermann P. (2022) Digital awakening for Germany. Deutsche Bank Researches. Available at: https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000525257/Digital_awakening_for_Germany%3A_Digital_Strategy_of.PDF (accessed: 20.11.2022)

9. Kraft C. et al. (2021) The digital transformation of Swiss small and medium-sized enterprises: insights from digital tool adoption. *Journal of Strategy and Management*, no. 2. Available at: 10.1108/JSMA-02-2021-0063 (accessed: 16.11.2021)

10. Savina N.V., Buryakova A.O. (2022) Audit of federal budget expenses on digitalisation. *Ekonomika stroitelstva*=Economics of Construction, no. 1, pp. 19–30 (in Russ.)

11. Tikhomirov Yu. A. et al. (2021) Law and digital information. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, no. 2, pp. 4–23 (in Russ.)

12. Transformation and digitalization of regulating social relations in modern realities and pandemic conditions (2020) Kazan: Otechestvo, 415 p. (in Russ.)

13. Tranos E., Kitsos T., Ortega-Argilés R. (2020) Digital economy in the UK: regional productivity effects of early adoption. *Regional Studies,* vol. 55, pp. 1924–1938.

14. Ulyanov A. Yu. (2022) Digital transformation of municipal administration: ways to optimize and evaluate efficiency. *Informatcionnoye obshhestvo*=Information Society, no. 2, pp. 43–52 (in Russ.)

15. Zaloilo M.V. (2019) The forward-looking nature of law-making and synchronisation of legal regulation. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 9, pp. 20–29 (in Russ.)

16. Zubarev S.M. (2020) Legal risks of digitalising public administration. *Actualnye voprocy rossiyskogo prava*=Current Issues of Russian Law, vol. 15, no. 6, pp. 23–32 (in Russ.)

Information about the author:

D.A. Shevelko — Senior Lecturer, Candidate of Sciences (Law).

The article was submitted to the editorial office 07.11.2022; approved after reviewing 30.11.2022; accepted for publication 30.11.2022.

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.

Вопросы права **В ЦИФРОВУЮ ЭПОХУ**

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

«Вопросы права в цифровую эпоху» — научный ежеквартальный электронный журнал, направленный на всесторонний анализ права в цифровую эпоху. Его главная цель заключается в рассмотрении вопросов, связанных с правовыми последствиями постоянно меняющихся информационных технологий.

Цифровая эпоха — это эпоха информационных и коммуникационных технологий, обусловливающих дальнейшее общественное развитие, в том числе с использованием цифровых данных. Но вместе с тем цифровое развитие выявляет пробелы в праве и потребность в новых правовых решениях.

“Вопросы права в цифровую эпоху” — журнал, который предоставляет возможность юристам — ученым и практикам — обмениваться мнениями. В том числе журнал поощряет междисциплинарные дискуссии по темам, находящимся на стыке права, технологий, экономики и политики в современном мире.

“Вопросы права в цифровую эпоху” — рецензируемый журнал. В нем применяется двойное “слепое” рецензирование присылаемых материалов.

Журнал приглашает авторов присылать статьи, отражающие результаты научных исследований регулирования цифровой среды. Редакция приветствует теоретические и компаративистские подходы, исследование перспектив правового развития в различных странах.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и включен в реестр зарегистрированных средств массовой информации серия серия Эл № ФС77-83367

ISSN 2713-2749

Адрес редакции
Россия, 109028 Москва, Б. Трехсвятительский пер, 3,
офис 113
Тел.: +7 (495) 220-99-87
http://law-journal.hse.ru
e-mail: lawjournal@hse.ru

Legal Issues in the **DIGITAL AGE**

Вопросы права
В ЦИФРОВУЮ ЭПОХУ

Учредитель
Национальный исследовательский университет «Высшая школа экономики»

4/2022

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ ТОМ 3

Редакторская колонка

Статьи

Научная статья

УДК:340
DOI:10.17323/2713-2749.2022.4.4.13

ЭЛЕКТРОННОЕ ГОСУДАРСТВО: ПРАВОВЫЕ АСПЕКТЫ

Ирина Юрьевна Богдановская

Национальный исследовательский университет «Высшая школа экономики», 101000 Россия, Москва, Мясницкая ул., 20, ibogdanovskaya@hse.ru, ORCID: 0000-0002-6243-4301

Аннотация

Во вступительной статье анализируются общие правовые подходы к установлению правовых основ электронного государства. Электронное государство — комплексное явление. Для его изучения требуется междисциплинарный подход — технический, социологический, правовой. Именно такой подход позволяет вскрыть сущность данного явления. Однако каждый из междисциплинарных подходов требует отдельной разработки. В данном случае речь идет о правовом подходе. Он формируется исходя из тех меняющихся социальных отношений, которые формируются под влиянием информационно-коммуникационных технологий. Правовой анализ в свою очередь сводится к формально-логическому, историческому, сравнительно-правовому методам. Формально-логический метод позволяет проанализировать законодательство, обеспечивающее развитие электронного государства. Исторический метод направлен на раскрытие эволюции законодательства в цифровую эпоху. Особое значение имеет сравнительный метод. Он позволяет показать общие и особенные тенденции правового обеспечения электронного государства в странах с разными правовыми и политическими традициями. В статье показано, как электронное государство восприняло традиции предшествующего развития, когда государство сформировалось как конституционное, правовое, социальное. В новых условиях имеет место поиск содержания новых правовых принципов, в частности принципа цифрового равенства, технической нейтральности. Их развитие идет сложным путем — от однозначного утверждения к критике и отрицанию. Примечательно, что такое развитие проходит в краткий период, зачастую порядка двух-трех десятилетий. В настоящем номере журнала содержатся отдельные материалы XI Международной конференции «Право в цифровую эпоху», проведенной в 2022 году при информационной поддержке журнала. В рамках конференции работала секция на тему «Электронное государство: правовая модель России и Индии». В номере поднимаются вопросы государственного управления в цифровую эпоху (Л.К. Терещенко. «Государственное регулирование и дерегулирование (на примере отрасли связи)»; Н.А. Данилов. «Трансформация электронного правительства и

электронного государственного управления в условиях цифровой экономики в России и за рубежом», Д.А. Шевелько. «Цифровизации в России: поиск правовой модели», А.С. Лолаева. «Электронная демократия: конституционно-правовое измерение»). Освещены правовые аспекты развития платформ (Н.А. Афифи, Р. Сони. «Онлайновые платформы как капитал и культурный код: изменяющаяся парадигма»).

Ключевые слова
государство, электронное государство, социальные отношения, правовые основы, информационно-коммуникационные технологии, междисциплинарный подход.

Для цитирования: Богдановская И. Ю. Электронное государство: правовые аспекты // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 4–13 (на англ. яз.)

Информация об авторе:
И.Ю. Богдановская –профессор, доктор юридических наук.

СТАТЬИ

Научная статья

УДК: 347, 342, 349.6
DOI:10.17323/2713-2749.2022.4.14.33

ОНЛАЙНОВЫЕ ПЛАТФОРМЫ КАК КАПИТАЛ И КУЛЬТУРНЫЙ КОД: ИЗМЕНЯЮЩАЯСЯ ПАРАДИГМА

Н.А. Афифи[1], Р. Сони[2]
[1] Университет Дж. Неру, Центр исследований научной политики, Нью Мераули Роуд, 136, Нью Дели 110067, Индия.
[2] Университет Дж. Неру, Центр исследований научной политики, Нью Мераули Роуд, 136, Нью Дели 110067, Индия.
[1] nabil58_sse@jnu.ac.in
[2] reetasony@mail.jnu.ac.in

Аннотация
Целью статьи является рассмотрение понятия платформ как инфраструктуры и их особенности в городских пространствах. В статье подчеркивается распространение онлайн-платформ доставки продуктов питания в городах и факторы, которые ускорили их внедрение и развитие. Кроме того, в статье предпринята попытка пролить свет на множественность алгоритмов путем разделения онлайн-платформ на отдельные алгоритмические компоненты. Такой подход к анализу платформ способствует пониманию различных способов, которыми алгоритмы этих платформ влияют на пользователей. Наконец, в статье освещаются различные способы управления онлайн-платформами в

городских пространствах. Исследование показывает, что хотя и платформы, и правительство устанавливают определенные гарантии прав пользователей, им не хватает стратегических усилий в области технологических инноваций.

Ключевые слова
агрегатор, алгоритмы, платформы, ответственность посредников, трудовое право, городские пространства.

Для цитирования: Афифи Н.А., Сони Р. Онлайновые платформы как капитал и культурный код: изменяющаяся парадигма // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 14–33 (на англ. яз.)

Информация об авторе:
Н.А. Афифи — аспирант.
Р. Сони — доцент, PhD.

Научная статья

УДК:340
DOI:10.17323/2713-2749.2022.4.34.51

ПРАВО НА ИНФОРМАЦИОННОЕ САМООПРЕДЕЛЕНИЕ: НА ГРАНИ ПУБЛИЧНОГО И ЧАСТНОГО

Эльвира Владимировна Талапина
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, 119571 Россия, Москва, проспект Вернадского, 82, talapina@mail.ru, https://orcid.org/0000-0003-3395-3126

Аннотация
Право на информационное самоопределение как право человека самостоятельно решать, когда и в каких пределах его персональные данные могут быть раскрыты, сформулировано в немецкой юриспруденции и стало моделью как для многих государств, так и для общеевропейского законодательства в целом. Оно рассматривается в качестве необходимого инструмента поддержания живой демократии, исходя из того, что частная жизнь является составной частью общества. Отправной точкой в судебном решении послужила кантовская теория моральной автономии личности. Это объясняет тесную связь судебной аргументации с правами человека и их публично-правовой охраной. Одновременно, под англосаксонским влиянием, развивается «имущественный подход» к персональным данным, которые могут стать объектом сделок. В рамках «имущественного подхода» персональные данные рассматриваются как ценный товар, который может быть объектом сделок и операций с другими людьми посредством лицензий. На практике в последнее время доступ к персональным данным все чаще открывается в качестве встречного исполнения (возмещения) по контрактам на цифровой контент и в обмен на персонализированные услуги. Исследование пока-

зало, что в правовой защите данных существует множество переплетений публичного и частного (информационное самоопределение как субъективное публичное право требует оформления соответствующих обязанностей государства, нет однозначной отраслевой квалификации согласия лица на обработку данных, отмечается недостаточность принципа конфиденциальности по умолчанию перед потенциальной возможностью причинения вреда). Анализ эволюции правовой защиты данных приводит к выводу о постепенном нивелировании разделения права на публичное/частное. Похоже, проблему обращения и защиты персональных данных невозможно решить в отраслевых рамках, а только комплексно, не нарушая при этом традиционной логики публичного и частного. Это означает, что право на информационное самоопределение, ввиду комплексного характера, можно расценивать как принцип, имеющий межотраслевой характер, который распространяется и на публично-правовую защиту данных, и на реализацию субъективного гражданского права в данной сфере.

Ключевые слова
персональные данные; цифровизация; частная жизнь; конфиденциальность; обработка данных; права человека.

Для цитирования: Талапина Э.В. Право на информационное самоопределение: на грани публичного и частного // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 34–51 (на англ. яз.)

Благодарность
Исследование проводилось в рамках НИР государственного задания РАНХиГС при Президенте Российской Федерации

Информация об авторе:
Э.В. Талапина — доктор юридических наук, доктор права (Франция), ведущий научный сотрудник.

Научная статья
УДК: 342
DOI:10.17323/2713-2749.2022.4.52.66

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ И ДЕРЕГУЛИРОВАНИЕ (НА ПРИМЕРЕ ОТРАСЛИ СВЯЗИ)

Людмила Константиновна Терещенко
Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 117218 Россия, Москва, Большая Черемушкинская ул., 34

Аннотация
Анализируются вопросы соотношения государственного регулирования и дерегулирования в сфере связи. Правовое регулирование такой важной

отрасли, как связь, должно отвечать современным вызовам. В настоящее время, когда стоит задача формирования современной цифровой экономики и снижения административных барьеров, вопросам соотношения государственного регулирования и дерегулирования в сфере связи уделяется особое внимание. Статья посвящена анализу правового регулирования в сфере связи, выявлению сфер, которые могут быть исключены из сферы государственного регулирования или же могут выиграть от саморегулирования и дерегулирования. Цель исследования — определить (на основе анализа) тенденции в государственном использовании регулирования и дерегулирования в сфере связи. С этой целью были исследованы возможные направления дерегулирования связи; проверены сферы, которые подверглись более интенсивному регулированию, и те, которые могли бы извлечь выгоду как из регулирования, так и из дерегулирования. В то время как сфера связи постоянно развивается и многие технологические аспекты этой сферы совершенствуются, возникают новые социальные отношения, которые на сегодняшний день не охвачены правовым регулированием и не подлежат дерегулированию. Таким образом, в статье рассматриваются вопросы правовых пробелов. Методология статьи представляет собой сочетание методов научного познания. В статье применены общенаучные и специальные методы исследования, в том числе формально-юридические. В заключении обобщаются результаты в виде кратких выводов.

Ключевые слова
сфера связи, телекоммуникации, государственное регулирование, саморегулирование, дерегулирование, оператор связи.

Для цитирования: Терещенко Л.К. Государственное регулирование и дерегулирование (на примере отрасли связи) // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 52–66 (на англ. яз.)

Информация об авторе:
Л.К. Терещенко — главный научный сотрудник, доктор юридических наук, заслуженный юрист Российской Федерации

Научная статья

УДК: 342
DOI:10.17323/2713-2749.2022.4.67.87

ТРАНСФОРМАЦИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА И ЭЛЕКТРОННОГО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Никита Аркадьевич Данилов
Национальный исследовательский университет «Высшая школа экономики», 101000 Россия, Москва, Мясницкая ул., 20, ndanilov@hse.ru

Аннотация
Статья посвящена вопросам, связанным с развитием электронного правительства и электронного государственного управления в России и за рубежом. В современном обществе социальные отношения модернизируются под воздействием информационно-коммуникационных технологий. Происходящие изменения касаются и ряда аспектов функционирования государства. Преобразования затрагивают все три ветви государственной власти. Для органов исполнительной власти характерны наиболее существенные преобразования. Развитие электронного правительства происходит в государствах с различными политико-правовыми традициями. Меняется порядок оказания государственных и муниципальных услуг, повышается открытость исполнительных органов. Происходящие процессы требуют теоретического осмысления, в том числе для выработки комплексного подхода к правовому регулированию электронного правительства. В связи с этим необходимо принимать во внимание и анализировать зарубежный опыт построения электронного правительства, общие и особенные черты законодательства в данной сфере. Объектом исследования является электронное государственное управление и органы исполнительной власти в условиях информационного общества. Предмет исследования представляет собой правовые нормы, регулирующие электронное правительство как новое состояние исполнительных органов государственной власти в России и в зарубежных странах. В ходе исследования установлено, что формирование электронного правительства сопровождается трансформацией системы исполнительных органов государственной власти. Создаются надведомственные и межведомственные органы, к функциям которых относится координация действий других исполнительных органов государственной власти в сфере управления информационным обществом, выработка согласованной политики, контроль над другими органами исполнительной власти. Происходит централизация функций в сфере электронного государственного управления и развития электронного правительства.

Ключевые слова
электронное правительство; электронное государственное управление; цифровое государственное управление; законодательство; органы власти; государственные услуги.

Для цитирования: Данилов Н.А. Трансформация электронного правительства и электронного государственного управления в условиях цифровой экономики // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 67–87 (на англ. яз.)

Информация об авторе:
Н.А. Данилов — доцент, кандидат юридических наук.

Научная статья

УДК: 342.34
DOI:10.17323/2713-2749. 2022.4.88.105

ЭЛЕКТРОННАЯ ДЕМОКРАТИЯ: КОНСТИТУЦИОННО-ПРАВОВОЕ ИЗМЕРЕНИЕ

Альбина Славовна Лолаева
Горский государственный аграрный университет, 362040 Россия, Владикавказ, ул. Кирова, д. 37, mirag.8184@yandex.ru, ORCID**:** 0000-0002-9021-7531

Аннотация
В статье рассматриваются вопросы электронной демократии как инновационной формы демократии в России, взятой в конституционно-правовом измерении. Исследуется влияние процессов информатизации на право, меняющих облик, контент и способы правового воздействия на преобразуемую среду. Особое влияние цифровизация оказывает на отрасль конституционного права в силу уникальных особенностей конституционно-правового регулирования, исключительной роли конституционного права, интегрирующего правовую систему. Обосновывается необходимость исходя из конституционных реалий вопросы информации и информационных технологий в Конституции Российской Федерации отнести к совместному ведению Российской Федерации и ее субъектов. Обосновывается, что электронная демократия в ее конституционном измерении является объектом прежде всего конституционно-правового регулирования. Электронная демократия в качестве инструментального выражения демократии, как политического процесса, основанного на конституционном императиве о принадлежности всей власти народу, закономерно входит в содержание предмета конституционного права, основанного на отношениях демократии и народовластия. При этом народный суверенитета, как и другие виды суверенитета — национальный, государственный вырастает из суверенитета личности как совокупности прирожденных и неотъемлемых прав и свобод человека и гражданина, находящихся под усиленной государственной защитой. Эти права, включая их цифровое сопровождение, образуют традиционный и значимый объект конституционно-правового регулирования. Речь идет прежде всего о правах, реализуемых целиком или преимущественно в цифровых показателях, формирующих цифровой статус личности, которым предшествует конституционный принцип равенства, приобретающий в информационных правоотношениях качества равенства цифрового, как равного гарантированного доступа каждого к информационно-коммуникационным технологиям. К этим правам принадлежит конституционное право каждого на информацию**,** включающего свободу искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29 Конституции). Электронная демократия наряду с конституционным правом является также предметом информационного права как совокупности юридических норм, регулирующих общественные отношения в инфор-

мационной сфере. Отмечается, что информационное право основывается на конституционных посылах, характеризующих информационные основы конституционного строя Российской Федерации.

Ключевые слова
информатизация, цифровизация, право, конституционное право, информационное право, электронная демократия.

Для цитирования: Лолаева А.С. Электронная демократия: конституционно-правовое измерение // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 88–105 (на англ. яз.)

Информация об авторе:
А.С. Лолаева — доцент, кандидат юридических наук.

Научная статья

УДК:340
DOI:10.17323/2713-2749.2022.4.106.129

ЦИФРОВИЗАЦИЯ В РОССИИ: ПОИСКИ ПРАВОВОЙ МОДЕЛИ

Дмитрий Александрович Шевелько
Московский государственный университет им. М.В.Ломоносова, 119991 Россия, Москва, Ленинские горы, 1/13, shevelko@audit.msu.ru, https://orcid.org/0000-0003-1355-067X

Аннотация
Статья посвящена вопросам правового регулирования цифровизации в России. Автор поставил цель формирования научно-теоретических положений о текущем состоянии правового регулирования цифровизации в России и о направлениях ее совершенствования. В рамках цели решаются задачи измерения и оценки достаточности и адекватности правового регулирования, его сравнения с аналогичным опытом Великобритании, ФРГ, Швеции и Швейцарии. В настоящее время в России сформулирована национальная цель построения цифровой экономики. В соответствии с ней принята одноименная национальная программа, а также иные программные документы. Вместе с тем ранее фиксации данной цели в России было принято несколько документов стратегического планирования в данной области (стратегия и доктрина). Однако, как показал анализ, их положения лишь частично были приняты во внимание при формировании нынешнего правового регулирования. Фактически в 2017 году были поставлены одни цели, а в 2018 году уже другие. В работе изучены недостатки в правовом регулировании долгосрочных целей цифровизации, заключающиеся в низком качестве определения содержания мероприятий, в отсутствии поддающихся измерению действий при разработке правовых актов, а также в недостаточной прора-

ботанности структуры документов. Между тем в зарубежных странах применяются подходы, способствующие ясности и понятности стратегий цифровизации. В них, как правило, присутствует анализ входных точек, инвентаризация мероприятий во всех областях, определяются измеримые меры правового регулирования. Такие подходы к цифровизации целесообразно применить и в России. В дополнение к отмеченным недостаткам есть пробелы в регулировании отечественных государственных информационных систем (ГИС) и в документах стратегического планирования. Они связаны с определением стоимости создания ГИС, с открытостью информации, с оценкой эффективности мероприятий. В статье содержится предложение о необходимости формирования в нашей стране единой стратегии цифровизации, общего повышения качества правового регулирования. Пока что правовые недостатки в сфере цифровизации ведут к рискам недостижения ее целей и задач, а также к отставанию России от других стран.

Ключевые слова
цифровизация, ГИС, информационные системы, цифровая экономика, правовое регулирование, стратегия цифровизации, 242-й вид расходов.

Для цитирования: Шевелько Д. А. Цифровизация в России: поиски правовой модели // Вопросы права в цифровую эпоху. 2022. Т. 3. № 4. С. 106–129 (на англ. яз.)

Информация об авторе:
Д.А. Шевелько — старший преподаватель, кандидат юридических наук.

Articles

Comment

Articles

Comment

Book Review

Articles

Comment

АВТОРАМ

Требования к оформлению текста статей

Представленные статьи должны быть оригинальными, не опубликованными ранее в других печатных изданиях. Статьи должны быть актуальными, обладать новизной, содержать выводы исследования, а также соответствовать указанным ниже правилам оформления. В случае ненадлежащего оформления статьи она направляется автору на доработку.

Статья представляется в электронном виде в формате Microsoft Word по адресу: lawjournal@hse.ru
Адрес редакции: 109028, Москва, Б. Трехсвятительский пер, 3, оф. 113
Рукописи не возвращаются.

Объем статьи
Объем статей до 1,5 усл. п.л., рецензий — до 0,5 усл. п.л.

При наборе текста необходимо использовать шрифт «Times New Roman». Размер шрифта для основного текста статей — 14, сносок — 11; нумерация сносок сплошная, постраничная. Текст печатается через 1,5 интервала.

Название статьи
Название статьи приводится на русском и английском языке. Заглавие должно быть кратким и информативным.

Сведения об авторах
Сведения об авторах приводятся на русском и английском языках:

- фамилия, имя, отчество всех авторов полностью
- полное название организации — места работы каждого автора в именительном падеже, ее полный почтовый адрес.
- должность, звание, ученая степень каждого автора
- адрес электронной почты для каждого автора

Аннотация
Аннотация предоставляется на русском и английском языках объемом 250–300 слов.
Аннотация к статье должна быть логичной (следовать логике описания результатов в статье), отражать основное содержание (предмет, цель, методологию, выводы исследования).

Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает…»).

Исторические справки, если они не составляют основное содержание документа, описание ранее опубликованных работ и общеизвестные положения, в аннотации не приводятся.

Ключевые слова
Ключевые слова приводятся на русском и английском языках. Необходимое количество ключевых слов (словосочетаний) — 6–10. Ключевые слова или словосочетания отделяются друг от друга точкой с запятой.

Сноски
Сноски постраничные.
Сноски оформляются согласно ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления», утвержденному Федеральным агентством по техническому регулированию и метрологии. Подробная информация на сайте http://law-journal.hse.ru.

Тематическая рубрика
Обязательно — код международной клас-сификации УДК.

Список литературы
В конце статьи приводится список литературы. Список следует оформлять по ГОСТ 7.0.5-2008.

Статьи рецензируются. Авторам предоставляется возможность ознакомиться с содержанием рецензий. При отрицательном отзыве рецензента автору предоставляется мотивированный отказ в опубликовании материала.

Плата с аспирантов за публикацию рукописей не взимается.

Выпускающий редактор *Р.С. Рааб*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*