ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 1, No. 2, 2020

ESSAYS

ARTICLES

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 1, No. 2, 2020

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 1, № 2, 2020

Contents

Essays

Articles

Содержание

Эссе

Статьи

DIGITAL LAW JOURNAL

AIMS AND SCOPE

The purpose of the Digital Law Journal is to provide a theoretical understanding of the laws that arise in Law and Economics in the digital environment, as well as to create a platform for finding the most suitable version of their legal regulation. This aim is especially vital for the Russian legal community, following the development of the digital economy in our country. The rest of the world has faced the same challenge, more or less successfully; an extensive practice of digital economy regulation has been developed, which provides good material for conducting comparative research on this issue. Theoretically, "Digital Law" is based on "Internet Law", formed in English-language scientific literature, which a number of researchers consider as a separate branch of Law.

The journal establishes the following objectives:

- Publication of research in the field of digital law and digital economy in order to intensify international scientific interaction and cooperation within the scientific community of experts.
- Meeting the information needs of professional specialists, government officials, representatives of public associations, and other citizens and organizations; this concerns assessment (scientific and legal) of modern approaches to the legal regulation of the digital economy.
- Dissemination of the achievements of current legal and economic science, and the improvement of professional relationships and scientific cooperative interaction between researchers and research groups in both Russia and foreign countries.

The journal publishes articles in the following fields of developments and challenges facing legal regulation of the digital economy:

1. Legal provision of information security and the formation of a unified digital environment of trust (identification of subjects in the digital space, legally significant information exchange, etc.).
2. Regulatory support for electronic civil turnover; comprehensive legal research of data in the context of digital technology development, including personal data, public data, and "Big Data".
3. Legal support for data collection, storage, and processing.
4. Regulatory support for the introduction and use of innovative technologies in the financial market (cryptocurrencies, blockchain, etc.).
5. Regulatory incentives for the improvement of the digital economy; legal regulation of contractual relations arising in connection with the development of digital technologies; network contracts (smart contracts); legal regulation of E-Commerce.
6. The formation of legal conditions in the field of legal proceedings and notaries according to the development of the digital economy.
7. Legal provision of digital interaction between the private sector and the state; a definition of the "digital objects" of taxation and legal regime development for the taxation of business activities in the field of digital technologies; a digital budget; a comprehensive study of the legal conditions for using the results of intellectual activity in the digital economy; and digital economy and antitrust regulation.
8. Legal regulation of the digital economy in the context of integration processes.
9. Comprehensive research of legal and ethical aspects related to the development and application of artificial intelligence and robotics systems.
10. Changing approaches to training and retraining of legal personnel in the context of digital technology development; new requirements for the skills of lawyers.

The subject of the journal corresponds to the group of specialties Legal Sciences 12.00.00 and Economic Sciences 08.00.00 according to the HAC nomenclature.

The journal publishes articles in Russian and English.

FOUNDER, PUBLISHER:

Maxim I. Inozemtsev
76, ave. Vernadsky, Moscow, Russia, 119454

Founded:	The journal has been published since 2020
Frequency:	4 issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	ЭЛ № ФС 77-76948 of 9 Oct. 2019 (Roskomnadzor)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454, +7 (495) 229-41-78, digitallawjornal.org, dlj@digitallawjournal.org
Published online:	20 Jul. 2020
Copyright:	© Digital Law Journal, 2020
Price:	Free

REGION GROUP OF COMPANIES With support of REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

Цель электронного журнала «Цифровое право» (Digital Law Journal) — создание дискуссионной площадки для осмысления в научно-практической плоскости легализации цифровых технологий, особенностей и перспектив их внедрения в нормативно-правовое поле. Особенно остро эта задача стоит перед российским сообществом правоведов в связи с развитием цифровой экономики в нашей стране. С этой же задачей сталкивается и остальной мир, решая её более или менее успешно. В мире сформировалась обширная практика нормативного регулирования цифровой экономики, она даёт хороший материал для проведения сравнительных исследований по этой проблематике. В теоретическом плане «цифровое право» опирается на сформировавшееся в англоязычной научной литературе академическое направление «интернет-право», которое ряд исследователей рассматривают как отдельную отрасль права.

Задачами журнала являются:

- Публикация исследований в области цифрового права и цифровой экономики с целью интенсификации международного научного взаимодействия и сотрудничества в рамках научного сообщества экспертов.
- Удовлетворение информационных потребностей специалистов-профессионалов, должностных лиц органов государственной власти, представителей общественных объединений, иных граждан и организаций в научно-правовой оценке современных подходов к правовому регулированию цифровой экономики.
- Распространение достижений актуальной юридической и экономической мысли, развитие профессиональных связей и научного кооперативного взаимодействия между исследователями и исследовательскими группами России и зарубежных государств.

В журнале публикуются статьи по следующим направлениям развития и задачам, стоящим перед нормативным регулированием цифровой экономики.

1. Нормативное обеспечение информационной безопасности, формирование единой цифровой среды доверия (идентификация субъектов в цифровом пространстве, обмен юридически значимой информацией между ними и т. д.).
2. Нормативное обеспечение электронного гражданского оборота; комплексные правовые исследования оборота данных в условиях развития цифровых технологий, в том числе персональных данных, общедоступных данных, “Big Data”.
3. Нормативное обеспечение условий для сбора, хранения и обработки данных.
4. Нормативное обеспечение внедрения и использования инновационных технологий на финансовом рынке (криптовалюты, блокчейн и др.).
5. Нормативное стимулирование развития цифровой экономики; правовое регулирование договорных отношений, возникающих в связи с развитием цифровых технологий. Сетевые договоры (смарт-контракты). Правовое регулирование электронной торговли.
6. Формирование правовых условий в сфере судопроизводства и нотариата в связи с развитием цифровой экономики.
7. Обеспечение нормативного регулирования цифрового взаимодействия предпринимательского сообщества и государства; определение «цифровых объектов» налогов и разработка правового режима налогообложения предпринимательской деятельности в сфере цифровых технологий. Цифровой бюджет; комплексное исследование правовых условий использования результатов интеллектуальной деятельности в условиях цифровой экономики. Цифровая экономика и антимонопольное регулирование.
8. Нормативное регулирование цифровой экономикой в контексте интеграционных процессов.
9. Комплексные исследования правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники.
10. Изменение подходов к подготовке и переподготовке юридических кадров в условиях развития цифровых технологий. Новые требования к навыкам и квалификации юристов.

Тематика журнала соответствует группе специальностей «Юридические науки» 12.00.00 и «Экономические науки» 08.00.00 по номенклатуре ВАК.

В журнале публикуются статьи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

Иноземцев Максим Игоревич
119454, Россия, Москва, просп. Вернадского, 76

История издания журнала:	Журнал издается с 2020 г.
Периодичность:	4 выпуска в год
Префикс DOI:	10.38044
ISSN online:	2686-9136
Свидетельство о регистрации средства массовой информации:	№ ФС 77-76948 от 09.10.2019 (Роскомнадзор)
Условия распространения материалов:	Контент доступен под лицензией Creative Commons Attribution 4.0 License
Редакция:	119454, Россия, Москва, просп. Вернадского, 76, +7 (495) 229-41-78, digitallawjournal.org, dlj@digitallawjournal.org
Дата публикации:	20.07.2020
Копирайт:	© Цифровое право, 2020
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2020-1-2-8-16

ESSAYS

DIGITAL TRANSFORMATION VS. COVID-19: THE CASE OF JAPAN

Junzo Iida

Soka University
1-236, Tangi-cho, Hachioji, Tokyo, Japan, 192-8577

Abstract

Whilst the DX policy of the Japanese government started in 2001, then called the E-Japan Strategy and being replaced a few years later by the *i*-Japan Strategy, in the 20 years since then IT has not been a success in Japan's administrative system. On the other hand, the private sector, concerned about Japan's lagging in its adoption of information technology, has been gradually moving forward to DX measures, such as electronic contracts. Then, this year, the COVID-19 pandemic broke out. Japan is (as of July 2020) about to experience a second wave of this disease. The need for DX has become imperative in all aspects of Japanese society, especially the government and business sectors. In the first half of 2020, the government set up DX policy rapidly; for example, civil court proceedings, the traditional carve seals custom, and the submission of administrative documents to government agencies have also been forced to move forward to DX due to COVID-19. It might be said that the crisis has been the catalyst for Japan's shift to DX. However, it will be at least a few years before it can be known whether Japan's DX will succeed, looking at the past examples within the Japanese bureaucratic system and politicians' attitudes towards DX.

Keywords

DX, digital transformation, digitalization, digital currency, Japanese government, Coronavirus, COVID-19, Japanese law, digital law

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Iida, J. (2020). Digital transformation vs. COVID-19: The case of Japan. *Digital Law Journal, 1*(2), 8–16. https://doi.org/10.38044/2686-9136-2020-1-2-8-16

Submitted: 11 Jun. 2020, accepted: 13 Jul. 2020, published: 20 Jul. 2020

ЭССЕ

ЦИФРОВИЗАЦИЯ И COVID-19: ОПЫТ ЯПОНИИ

Д. Иида

Университет Сока
192-8577, Япония, Токио, Тангичо, Хатиодзи, 1-236

Аннотация

Правительство Японии в 2001 году взяло курс на политику цифровой трансформации (E-Japan Strategy, впоследствии — *i*-Japan Strategy). Тем не менее за последние 20 лет информационные технологии так и не были успешно внедрены в систему государственного управления. В то же время частный сектор, обеспокоенный отставанием Японии в этой области, инициативно внедряет цифровые механизмы, одним из примеров которых служат смарт-контракты. В начале 2020 года мир столкнулся с пандемией COVID-19, в настоящее время в Японии ожидается вторая волна. Потребность в цифровой трансформации становится актуальной во всех сферах японского общества, особенно в государственном управлении и бизнесе. В первой половине 2020 года правительство приступило к реализации цифровой повестки: нововведения коснулись гражданского процесса, подачи документов в органы государственной власти, а также таможенных процедур. Таким образом, кризис ускорил процесс внедрения цифровых технологий в право Японии. Учитывая осторожный, консервативный подход отдельных политиков, потребуется минимум несколько лет чтобы оценить успешность цифровой модели японского общества.

Ключевые слова

цифровая трансформация, переход к цифровой экономике, цифровизация, цифровая валюта, правительство Японии, коронавирус, COVID-19, право Японии, цифровое право

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Иида, Д. (2020). Цифровизация и COVID-19: опыт Японии. *Цифровое право*, *1*(2), 8–16. https://doi.org/10.38044/2686-9136-2020-1-2-8-16

Поступила: 11.06.2020, принята в печать: 13.07.2020, опубликована: 20.07.2020

Introduction

As of July 2020, Japan is in the midst of the turmoil of battling COVID-19. The numbers of infected persons have risen since lifting the Declaration of National Emergency on 25 May. PCR testing is limited to the person who is seriously ill or gets special permission for this test. Compared with countries such as Korea, China, and the U.S.A., the numbers of PCR testing are remarkably limited, seemingly controlled by the Ministry of Health, Labour and Welfare, to about 17,354 nationwide as of 31 July[1], and 4,851 per day in Tokyo Metropolitan as of 30 July[2]. This crisis, happening so suddenly in early 2020, has pushed the Digital Transformation (hereafter, DX) movement all across the country forward, especially for the Japanese government, which has been moving toward DX gradually. Indeed, *the Nihon Keizai Shimbun,* a famous economic newspaper in Japan, ran an article subtitled "Twenty Years, the Japanese Government Tried to Become an IT Nation, but Failed" (Yasoshima, 2020). DX in Japan arguably started in 2001, when the Japanese government adopted a national plan of DX, called the E-Japan Strategy[3]. In July 2009, *i*-Japan Strategy 2015 was announced, which was intended to be completed by 2015 and seemed to be a revised plan for E-Japan Strategy[4].

Since then, policies and plans were made, but they seem not to have fully succeeded. This is because it has been thought that promoting the DX policy as a campaign pledge is not a way for lawmakers or the ruling party to win elections (Yasoshima, 2020). Whether this analysis is correct or not needs to be analyzed more, but it may be that politicians usually focus on subjects that will win them votes in elections; DX policy was not in such a criterion.

The coronavirus outbreak has dramatically turned these circumstances upside down. Japan is now in a situation where it is necessary to push forward its DX policy. The government, led by the Liberal Democratic Party (LDP), is beginning to see that the DX policy will hold one of the critical elements to the House of Representatives elections scheduled for the next year (though perhaps these might happen in the fall of 2020).

On the part of Japanese bureaucracy, DX is recognized to have accelerated. In April 2020, the Minister of Justice told the press that to promote the digitalization of legal administration and the adoption of AI and ICT, the Minister was invited to participate in the Ministry of Justice Web-meeting. The Minister said that the Ministry of Justice Web-meeting would be held periodically. On the other hand, the Minister admitted that the Ministry of Justice currently had a video-meeting system with a line that did not connect to any place other than in the Ministry, which was a big problem intended to be solved soon. The comment of the Minister reflects the fact that there is a problematic tradition in bureaucratic sections. It might be said that the coronavirus outbreak forced these bureaucratic organizations to the realization that digital transformation must be advanced.

In short, due to this coronavirus pandemic, it has become more apparent that Japan has now entered a new era in which the DX process must be fast-tracked. The author would like to describe current measures for DX that the Japanese government has been tackling.

---

1 Ministry of Health, Labour and Welfare. (2020, June 30). *Situation update for COVID-19 and the MHLW's response.* https://www.mhlw.go.jp/stf/covid-19/ kokunainohasseijoukyou.html

2 Tokyo Metropolitan Government. (2020, June 30). *Updates on COVID-19 in Tokyo*. https://stopcovid19.metro.tokyo.lg.jp/en

3 IT Strategic Headquarters. (2001, January 22). *E-Japan Strategy*. https://japan.kantei.go.jp/it/network/0122full_e.html

4 IT Strategic Headquarters. (2009, July 6). *I-Japan Strategy: Striving to create a citizen-driven, reassuring & vibrant digital society towards digital inclusion & innovation*. https://japan.kantei.go.jp/policy/it/i-JapanStrategy2015_full.pdf

Recent DX Policies of the Japanese Government

DX policies of the Japanese government are currently being planned and implemented by several organs. The Ministry of Economy, Trade and Industry (METI) has taken the lead in formulating and promoting policies for DX in economic and industrial sectors. The Expert Group for Digital Transformation was established in May 2018 within METI, and this unit has researched various issues of DX and examined countermeasures: *The DX Report — Overcoming the IT System, "the Cliff of 2025" and the Full-Scale Development of DX,* was published in September 2018[5]. In July 2018, METI set up a small team called the DX Office. Its mission is to lead the digitalization of the procedure of the public administration alongside the DX movement of the Japanese government as a whole[6]. Pursuing a concrete measure, the Ministry METI formulated the *DX Promotion Indicators and Guidance for Promoting Digital Transformation* to clarify these issues; it says that executives should be aware of and to help boards of directors and shareholders review DX initiatives (Ministry of Economy, Trade and Industry, 2019).

COVID-19 has accelerated these movements for DX. The IT Strategic Headquarters, and the National Center of Incident Readiness and Strategy for Cybersecurity, both belong to the Cabinet, formulated basic government policy in 2020. On 27 April 2020, the "Intellectual Property Promotion Plan 2020" (hereafter, IP2020) was adopted by the Japanese government. It is a plan to promote digitalization through intellectual property. Section 3 of IP2020 is titled "Promoting the Strategic Use of Intellectual Property in the Innovation Ecosystem", saying that DX should be accelerated[7].

A further step for DX taken in 2020 is the proposal, put forwards by the special committee for promotion of the digital society of the Liberal Democratic Party (LDP), of the establishment of a ministry to promote DX. Moreover, a new organization for the digitalization of public administration was proposed by the LDP's Economic Growth Strategy Headquarters.

Not more than a month later, this proposal was swiftly crystalized as a government policy; on 17 July 2020, the Cabinet Office officially announced the cabinet decision "the Basic Policy of Economic and Fiscal Management and Reform 2020" (hereafter "the Basic Policy 2020"). The Basic Policy 2020 consists of three chapters: Chapter 1: Overcoming the Crisis Under New Coronavirus Infections and the New Future Ahead; Chapter 2: Responding to the Spread of Infectious Diseases and Phasing Out Economic Activities; and Chapter 3: Realizing the "New Normal". In particular, Chapter 3 stressed that the intensive investment in and implementation of digitalization would be a driving force for the "new normal" age, called the Digital New Deal. In this chapter, regarding decisive action about digital government, promoting Digital Transformation is particularly mentioned. It also says that the Japanese custom of using paper documents, stamping carved seals, and face-to-face meetings should be reexamined.

---

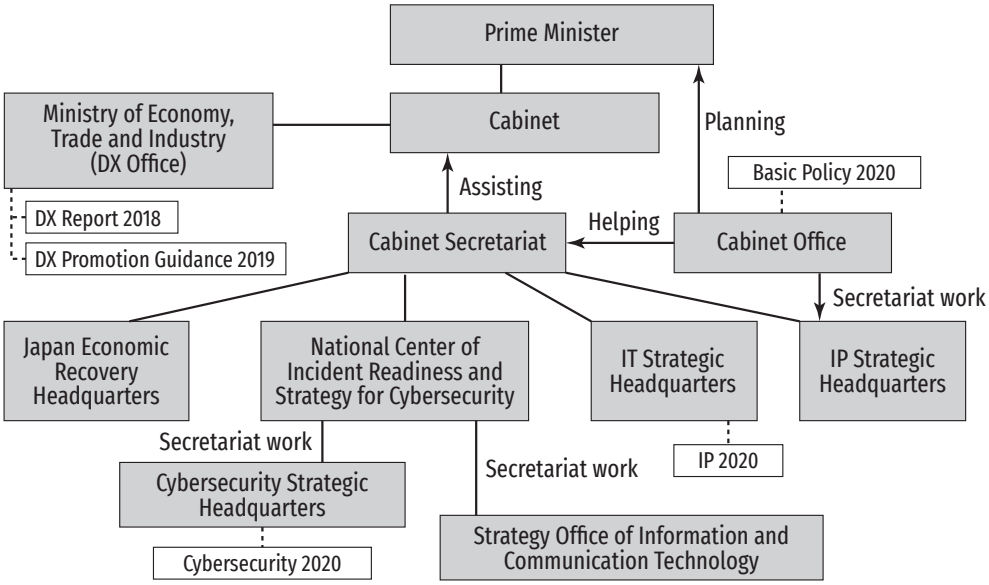
5 Ministry of Economy, Trade and Industry (2018). Repōto— IT shisutemu' 2025 nen no gake' no kokufuku to DX no honkaku-teki na tenkai [*DX Report — Overcoming the IT System, «the Cliff of 2025,» and the Full-Scale Development of DX*]. https://www.meti.go.jp/press/2018/09/20180907010/20180907010-3.pdf

6 Ministry of Economy, Trade and Industry (2018). Keizai sangyō-shō no dejitaru-ka o suishin suru' keizai sangyō-shō oyobi chū shō kigyō chō dejitaru. toransufōmeishon-shitsu' o secchi shimasu [Ministry of Economy, Trade and Industry establish «Ministry of Economy, Trade and Industry and Small and Medium Enterprise Agency Digital Transformation Office» to promote digitalization]. https://www.meti.go.jp/press/2018/07/20180725002/20180725002.html

7 IP Strategic Headquarters (2020). Chiteki zaisan suishin keikaku ni rei ni rei— shingata korona-go no' nyū. nōmaru' ni muketa chizai senrya ku [Intellectual Property Promotion Plan 2020 — Intellectual property strategies for the «new normal» post-new coronavirus]. https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20200527.pdf

Figure 1

The Administrative Structure and Comprehensive Plans for DX Policy



Note. Illustrated by the author, based on websites of each relevant organization of the Japanese administration system.

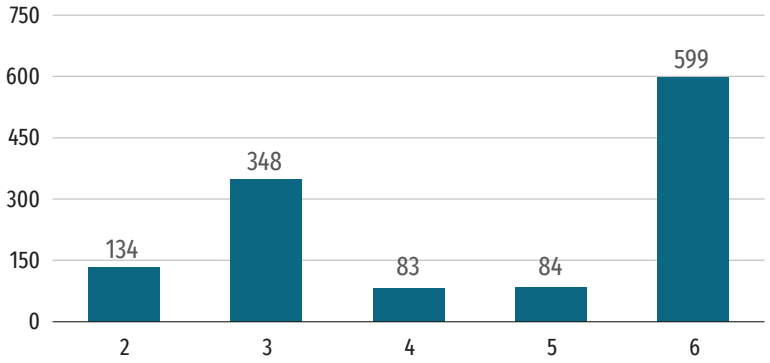
The Basic Policy 2020 further points out that "looking at the recent implementation of support measures in response to the infectious disease, it is clear that digitalization and online system are lagging behind, especially in the administrative sector". Regarding Digital New Deal, the Basic Policy 2020 declares that the Japanese government will actively promote the digitalization of Japanese society as a whole. It also indicates that building a digital government would be the highest priority policy issue, and that promoting DX in the private sector and creating an environment that encourages investment and innovation in private sectors should proceed. Meanwhile, the Basic Policy admits that the digitalization of public administration is lagging, and emphasizes the need for intensive reformation and acceleration of the digital government for the entire government. It says that concentrating on standardization and sharing business processes and information systems among national and local governments is also needed, adding that the development of digitalization and cloud computing of the local governments, through cooperation between the government and the private sector, is essentially important.

On 15 July 2020, the Japanese government held a joint meeting of IT Strategic Headquarters, headed by the Prime Minister, and decided a Declaration regarding Creation of World's Most Advanced Digital Nation, aiming for the digitalization of the whole of Japanese society. This Declaration was officially announced on 17 July 2020[8].

[8] Cabinet Office. (2017, May 30). *Declaration to be the World's most advanced IT nation basic plan for the advancement of public and private sector data utilization*. Prime Minister of Japan and His Cabinet. https://japan.kantei.go.jp/policy/it/2017/20170530_full.pdf

Figure 2

The Numbers of Web-Conferencing



Note. Created by the author.

Two days later, after the announcement was publicized, the government's Cyber Security Strategic Headquarters issued a new plan, "Cybersecurity 2020". Although it is only a guideline with no legal effect, it aims to encourage government agencies and private enterprises to carry out digital transformation. To promote DX in Japan, the government demanded that all parties take positive cyber defense to prepare for potential attacks.

It remains to be seen whether all of these policies will be successfully implemented, and whether Japan will be able to join the ranks of advanced IT countries. Also, the reformation of administrative tradition — the so-called vertical administration system — seems to be one of the critical elements for Japan's DX success.

DX and the Litigation Procedures in Civil Courts

On the part of the judicial sector, the Office of the Supreme Court in Japan announced using IT tools to sort out issues, such as web conferencing, as a first step in introducing IT into civil litigation procedures. Eight district head courts out of fifty district head courts across the country, including some division of the Tokyo and Osaka District Courts and an Intellectual Appeal Court, would be expected to introduce web conferencing[9]. As of 6 July, fourteen district courts nationwide have already started web-conferencing[10].

However, in April and May, the numbers of web-conferencing decreased because of the Declaration of National Emergency for COVID-19. After the Declaration was lifted, this number increased, as shown in the graph below.

[9] Supreme Court of Japan (2020). Webu kaigi-tō noIT tsūru o katsuyō shita sōten seiri no un'yō no kaishi ni tsuite [Regarding the start of the operation for legal issue arrangement using IT tools such as web conferencing]. Courts in Japan. https://www.courts.go.jp/about/topics/webmeeting_2020_0203/index.html

[10] Supreme Court of Japan (2020). Webu kaigi-tō noIT tsūru o katsuyō shita sōten seiri no un'yō o kaishi shite iru chō ni tsuite [Regarding the courts that already started a new operation of the controversial arrangement using IT tools such as web conferencing]. Courts in Japan. https://www.courts.go.jp/about/topics/webmeeting_2020_0706/index.html

Web conferencing for sorting out issues is not open to the public. In the legal sphere, the advantages of IT-based court proceedings are now apparently due to the fact that attorneys can attend the meeting at each law firm. The Japanese government plans to amend the related laws to allow for oral arguments via web conferencing in 2023 and online submission procedures of complaints in 2025.

From Carved Seals to Electric Seals

Carved seals (hanko or inkan in Japanese) are used in all aspects of daily life in Japan, such as receiving a parcel delivery service, making a notification at a bank, or receiving something at a post office. It is so common that when people get married, their friends and parents give them a high-grade carved seal made of blackwood or a similar material for their private seals as a gift to make Jitsu-in (meaning an officially registered carved seal). This is required when borrowing a loan or buying real estate, for example. A carved seal — especially a registered carved seal — is required in the business world to make contracts. It can be said that a carved seal is a part of Japanese customs, even a culture. A few cases have taken place where a challenge has been made so as to avoid such a custom[11]. This kind of custom has been considered necessary for official administrative procedures. A carved seal is required in court proceedings and ordinary governmental affairs as well.

However, COVID-19 seems to have made Japanese society dramatically pay attention to the fact that the carved seal may be unnecessary. The demand for electronic contract services is increasing rapidly. Unlike traditional written contracts, electronic contracts do not involve printing, stamping, enclosing, or mailing the contract. It makes operations more efficient and reduces postage costs. Indeed, in June 2020, the government already issued a guideline on carved seals; it says that carved seals would not necessarily be required in contracts for private companies and public-private transactions to promote tele-work, And even if not stamped with a carved seal, it is possible to certify a contract by email texts and other digital documents, records of transmissions and receipts, and digital signatures.

On the part of the private sector, the trend for electronic contracts has now stopped. Fuji Xerox announced that it would sell an electric contract system nationwide. The Nomura Real Estate Development, one of the leading real estate companies, would positively introduce an electric contract system in winter 2020.

Considering the movement of introducing an electric contract system, the government announced another measure for its intention to promote DX policy. In the past, when a digital signature was made, a digital certificate had to be attached to the digital signature to verify that it was the person who made it. However, it took several weeks to obtain a digital certificate, which raised questions about its convenience. The government confirmed that digital signatures without a digital certificate would also be valid.

Based on these measures, further growth of the electronic contract service industry is expected. It may be said that this could lead to a new social phenomenon whereby a larger number of companies will use electronic contracts instead of paper documents with carved seals.

This trend was boosted by the fact that the Japanese government and four economic organizations have announced a joint declaration aimed at reducing the amount of paperwork, carved seal, and face-to-face work. These practices have continued for a long time due to Japanese legal systems and practices in corporate contracts and administrative procedures. Indeed, con-

[11] Nikkei BP Company. (2016). A case study: Japan mortgage loan company: Japan's first contract system without a registered seal: Breaking the barriers of business practices with wisdom and IT. *Nikkei Computer*, (925), 48–51.

trary to the private sector that remarkably introduced electric contracts, sixteen of twenty-one organizations of the Japanese government did not use electric contracts in the 2019 fiscal year[12].

A Recent Decision by the Japanese Supreme Court, Reflecting the Digital Age

Intellectual property rights, such as copyrights, are likely to pose various challenges in the digital transformation era. The recent decision of the Japanese Supreme Court seems to symbolize Japan's digital age. The outline of the case and the judgment are as follows[13].

A photographer (hereafter X) took a photo of a flower and posted it on his website. X put a copyright mark and X's name on the edge of the picture. A Twitter user saw this photo and posted it on Twitter without permission. Twitter users who saw this photo retweeted the photo, and in these cases, the part of the picture with X's name and copyright mark on it was automatically trimmed by Twitter's system. Alleging that the rights of attribution — one of the author's moral rights — had been violated, X claimed Twitter should disclose the email addresses of the users who retweeted the photo. However, the company refused to do so.

In 2016, the Tokyo District Court found copyright infringement by unauthorized tweets. However, it denied that retweet users infringed X's rights. On appeal, the Intellectual Property High Court found that the retweet users *had* violated X's right, and decided to disclose the email addresses of those people who retweeted. This time, the Supreme Court's decision upheld the Intellectual Property High Court's decision, requiring Twitter reveal its user's email addresses.

Interestingly, although all five of the judges made a unanimous decision, one judge added a dissenting opinion. The judge said that it presented too excessive a responsibility for the retweeters, since they did not know the photos were trimmed simply because Twitter automatically trimmed the photo. On the other hand, the presiding judge's additional comment is that retweeters who do not know about Twitter's trimming system might violate the right of attribution. Twitter has become one of the most critical information distribution tools in society today. It is not reasonable to entrust individual Twitter users to raise their awareness of the rights. Concerning the protection of attribution rights and the avoidance of burden on Twitter users, Twitter is expected to take appropriate measures regarding a provider of information distribution services' social responsibility, which has become an essential social infrastructure[14].

It can be said that the judges strictly interpreted the Copyright Act. The only way to protect the rights of the original author of the photo is to acknowledge the responsibility of the retweets. Nevertheless, the question remains. As the dissenting opinion says, the retweeters did not know the pictures were trimmed due to Twitter's automatic trimmed system. Since no comment has been made on this legal case, future analysis of this case by the legal scholars and digital experts should be expected.

---

12 Horigome, T. (2020, July 7). The public administration's electric contracts spent 1% last fiscal year, of the maintenance cost of 1.6 billion yen, a lack of progress in de-carved seals. *The Asahi Shimbun.* Retrieved from Kikuzo II database.

13 Abe, S. (2020). Trimming and reprinting the photographer's name is "infringement of rights" Supreme Court rules: beware of image retweets. *The Asahi Shimbun.* Retrieved from Kikuzo II database.

14 Supreme Court of Japan (2018). Heisei san rei nen (ju) dai ichi yon ichi ni gō hasshin-sha jōhō kaiji seikyū jiken-rei wa ninen shichi gatsu ni ichi nichi dai san shō hōtei hanketsu [Case Received in 2018, No. 1412 Caller Information Disclosure Request Case July 21, 3rd Small Court Judgment]. Courts in Japan. https://www.courts.go.jp/app/files/hanrei_jp/597/089597_hanrei.pdf

Digital transformation involves AI, Cloud, IoT, and Big Data. It should be added that it is vital that the laws and legislative policy, including interpretation of legal rules, also align with the DX era.

Conclusion

The author has illustrated current DX policies of the Japanese government, especially in the administrative and judicial sectors. A few cases should be added to understand to what extent Japan's current DX movement is underway. For instance, the government announced that it has begun studying the introduction of digital currencies. The Bank of Japan (BOJ) has already begun joint research with overseas central banks, and the government is now in line with the BOJ. The Bank of Japan said that it was the government that determines the issuance of digital currency.

Further movement of DX in Japan is seen in the so-called insurance-tech business. Tokio Marine & Nichido Fire Insurance Co. Ltd. has recently launched a new system in which AI analyzes the data of the drive recorder installed in a car and produces an accident investigation report. It previously took a week to create an accident investigation report, but it can be completed in 5 minutes by using this system (Fujimura & Hiramoto, 2020).

The Japanese government is facing a second wave of COVID-19 as of July 2020. Its policies for DX were in place in the first half of the year. Future historians may argue that 2020 was a turning point in history for the world and Japan. Under these circumstances, for Japan, 2020 will become the year when the digital transformation became indispensable. The private sector and the administrative sector are accelerating digitalization at all criteria and levels. It will become clear whether or not the Japanese digital transformation proves to be successful, perhaps within the next five to ten years.

Information about the author:

Junzo Iida — Ph.D., Professor of Law, Soka University, Tokyo, Japan.
iida@soka.ac.jp

Сведения об авторе:

Ида Д. — Ph.D., профессор права Университета Сока, Токио, Япония.
iida@soka.ac.jp

https://doi.org/10.38044/2686-9136-2020-1-2-17-27

ESSAYS

"REGULATORY SANDBOXES" IN RUSSIA: NEW HORIZONS AND CHALLENGES

Damir R. Salikhov

Lomonosov Moscow State University
1, Leninskie Gory, Moscow, Russia, 119991

Abstract

"Regulatory sandboxes" are regarded as a special mechanism for setting up experimental regulation in the area of digital innovation (especially in financial technologies), creating a special regime for a limited number of participants and for a limited time. Russia has its own method of experimental regulation, which is not typical but may be helpful for other jurisdictions. There are three approaches to legal experiments (including digital innovations) in Russia. The first approach is accepting special regulation on different issues. There are recent examples of special laws (e.g. Federal Law on the experiment with artificial intelligence technologies in Moscow). An alternative to this option is establishing experimental regulation by an act of the Government if legislation does not prohibit it (e.g. labeling with means of identification). The second approach deals only with Fintech innovations and provides a special mechanism to pilot models of innovative financial technologies. The participants of such a "sandbox" may create a close-to-life model in order to estimate the effects and risks. If the model works fine, the regulation may be amended. The third approach works with creating a universal mechanism of real-life experiments in the sphere of digital innovations based on the special Federal Law and the specific decision of the Government of the Russian Federation or the Bank of Russia in the financial sphere. The author compares the three approaches and their implementation within the framework of Russian legislation and practice and concludes that this experience may be used by developing countries with inflexible regulation, in order to facilitate the development of digital innovations.

Keywords

sandboxes, regulatory sandbox, digital innovation, legal experiment, Russian experience, digital law

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Salikhov, D. R. (2020). "Regulatory sandboxes" in Russia: New horizons and challenges. *Digital Law Journal, 1*(2), 17–27. https://doi.org/10.38044/2686-9136-2020-1-2-17-27

Submitted: 15 Apr. 2020, accepted: 23 Jun. 2020, published: 20 Jul. 2020

ЭССЕ

«РЕГУЛЯТИВНЫЕ ПЕСОЧНИЦЫ» В РОССИИ: НОВЫЕ ГОРИЗОНТЫ И ВЫЗОВЫ

Д.Р. Салихов

Московский государственный университет им. М.В. Ломоносова
119991, Россия, Москва, Ленинские горы, 1

Аннотация

«Регулятивные песочницы» рассматриваются как особый механизм экспериментального регулирования в области цифровых инноваций (в первую очередь в области финансовых технологий), который создает специальный правовой режим для ограниченного числа участников в течение определенного времени. В России представлен собственный способ подобного регулирования, который не является типичным, но может оказаться полезным для других государств. Так, существуют три соответствующих подхода к правовым экспериментам. Первый — введение специального правового регулирования. Речь идет об издании специальных законов (к примеру, Федеральный закон об эксперименте с технологиями искусственного интеллекта в Москве) либо установлении экспериментального регулирования подзаконным актом правительства (например, маркировка средствами идентификации). Второй подход касается только инноваций в сфере финансовых рынков и предоставляет специальный правовой режим для пилотирования моделей инновационных финансовых технологий. Участники такой «песочницы» могут создать приближенную к жизни модель для оценки последствий и рисков ее внедрения. Если модель будет функционировать оптимально, в правовое регулирование могут быть внесены соответствующие изменения. Третий подход касается создания универсального механизма реальных правовых экспериментов в сфере цифровых инноваций. Автор сопоставляет указанные подходы, используемые в Российской Федерации, и приходит к выводу, что этот опыт может оказаться полезным для развивающихся стран с довольно жестким регулированием в целях содействия развитию цифровых инноваций.

Ключевые слова

песочницы, регулятивная песочница, цифровые инновации, правовой эксперимент, российский опыт, цифровое право

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Салихов, Д. Р. (2020). «Регулятивные песочницы» в России: новые горизонты и вызовы. *Цифровое право, 1*(2), 17–27. https://doi.org/10.38044/2686-9136-2020-1-2-17-27

Поступила: 15.04.2020, принята в печать: 23.06.2020, опубликована: 20.07.2020

The idea of so-called "regulatory sandboxes" is not brand new; this approach is pretty common in the experimental regulation of digital innovations, especially fintech innovations.

A basic prerequisite for this institution is in the problem of the development of technologies happening faster than regulation (Fenwick & Wulf, 2017). Under these circumstances, the government is looking for ways to make regulation more flexible to assist with sustainable and effective development across different areas of the economy.

The motherland of "regulatory sandboxes" is the United Kingdom (the first "sandbox" was designed in 2016)[1].

The same mechanisms exist in the Unites States of America (Allen, 2019), Australia[2], Singapore[3], the United Arab Emirates[4], Hong Kong (Huang et al., 2020), Switzerland[5], Thailand[6], Indonesia[7], Republic of Kazakhstan[8], Bahrain[9], Jordan[10], Sierra Leone[11], and a few other countries.

According to mass media, at least eight countries are working on the same idea — Brunei, the People's Republic of China, India, Kenya, Mexico, Mozambique, Nigeria, and Pakistan.

This diverse mix of countries shows that specific countries with different legal and political traditions are interested in this institution. Undoubtedly, the list of countries will be broadened within a few years.

In general, the mechanism of "regulatory sandboxes" provides methods for testing new technologies and business processes within the limited number of participants, followed by special legal prescriptions, which means either cancelling assorted mandatory requirements for the purposes of experiments, or developing special requirements and "individual" provisions. Both of these options have a limited period, which is necessary for checking up the new technology or business processes, and the effects of their implementation.

---

1 Financial Conduct Authority. (2020, May 04). *Digital sandbox — coronavirus (Covid-19) pilot*. https://www.fca.org.uk/firms/innovation/digital-sandbox

2 Australian Securities & Investments Commission. (2017, December). Retaining ASIC's fintech licensing exemption (Consultation Paper No 297). https://asic.gov.au/for-business/innovation-hub/fintech-regulatory-sandbox/

3 Monetary Authority of Singapore. (n.d.). *Overview of regulatory sandbox*. https://www.mas.gov.sg/development/fintech/regulatory-sandbox

4 Fintechnews Middle East. (2019, March 11). *UAE regulator initiatives to bring fintech to the next level*. https://fintechnews.ae/3577/fintechdubai/uae-regulator-fintech-initiative-sandbox-cryptocurrency-ekyc-payments/

5 Balzli, T. (2019, July 01). FinTech license and sandbox — Adjustments to FINMA circulars 08/3 and 13/3. *PwC Switzerland*. https://www.pwc.ch/en/insights/regulation/Fintech-license-and-sandbox-adjustments.html

6 Gnanasagaran, A. (2018, February 22). Fintech sandboxes in Southeast Asia. *The ASEAN Post*. https://theaseanpost.com/article/fintech-sandboxes-southeast-asia

7 Nabila, M. (2018, August 21). *OJK launches "OJK Infinity", Digital Financial Innovation Center. Also releasing the latest regulation about Digital Financial Innovation (IKD)*. DailySocial. https://dailysocial.id/post/ojk-launches-ojk-infinitydigital-financial-innovation-center

8 The Astana Times. (2015, October 10). *Astana International Financial Centre to cement capital's place in global finance*. https://astanatimes.com/2015/10/ astana-international-financial-centre-to-cement-capitals-place-in-global-finance/

9 Crane, J., Meyer, L. M., & Fife, E. A. (2018, June). Thinking inside the sandbox: An Analysis of regulatory efforts to facilitate financial innovation. *RegTechLab*. https://www.regtechlab.io/report-thinking-inside-the-sandbox

10 AFI. (2018, April 2). *Policy forum in Jordan: FinTech as a key catalyst for financial inclusion*. https://www.afi-global.org/news/2018/04/ policy-forum-jordan-fintech-key-catalyst-financial-inclusion

11 Massally, T. K., & Duff, S. (2018, May 15). What can we learn from Sierra Leone's new regulatory sandbox? *CGAP*. https://www.cgap.org/blog/what-can-we-learn-sierra-leones-new-regulatory-sandbox

This mechanism is needed given the unpredictable consequences and risks herein, and is potentially useful for the business and social opportunities of using the testing technology or processes.

For instance, the state has some mandatory requirements for taxi drivers, including a daily medical checkup and a special type of driving license. These requirements cannot be applied for a drone taxi, which has no human driver within the car but may have a "driver" outside observing the entire processes. Prohibiting this type of taxi only on the basis of not corresponding to some mandatory requirements seems unreasonable, yet society may not ready to prescribe this or that regulation for this type of taxi without research and testing. Both horns of this dilemma show the difficulties herein.

Under these circumstances, and due to the fact, that with no practical experience it is impossible to establish adequate regulation for most innovations, the government is seeking ways of how to try the new approaches without fundamental changes of legislation.

"Sandboxes" are the perfect mechanism for these purposes, since they are a framework (not typical for other companies beside the current participants) set up by a regulator (e.g. a Central Bank in Fintech area) that allows "innovators" to conduct "live" experiments in a controlled environment under a regulator's supervision. In other words, this mechanism creates a controlled experiment, where the government and the participants are able to find the most balanced and fair legislation, minimizing the risks for public values and maximizing the positive effects.

Returning to the example of a drone taxi, the government may cancel some of the requirements and, at the same time, add other special requirements (e.g. for protecting pedestrians, for insuring liability including civil and criminal liability, for control of all drone taxis online, etc.) based on their risk analysis.

The metaphor of the "sandbox" is illustrative, as the entire experiment is limited to participants, technologies, applicable requirements, etc. Being under the supervision of the state, the "sandbox" may be converted on the basis of special regulations. Novel financial products, high technologies, and innovate business models or processes may be checked under a special set of norms, rules, and requirements, providing appropriate safeguards and protecting public interest.

This tool for the development of digital innovations is used in global practice (to a greater extent, it relates to the financial services market), and enables the reduction of the time and costs in introducing innovative products and improving the relevant regulatory legal framework. Due to the fact that, from time to time, current regulation does not fully consider new practices and use of new technologies, special legal regimes help to reduce legal uncertainty and legal risks for all participants.

In theory the idea is clear, but in practice there are many issues — tax policy, preventing of the risks for lives and health, the limits of converting the experimental regulation during the "sandbox" period, antitrust legislation, and so on.

Another issue is devoted to the areas of experimental regulation. Historically there was the only area — financial technologies (Bromberg et al., 2017). However, some countries extended the mechanism to digital innovations in general (Wechsler et al., 2018).

In fact, there is not a commonly accepted notion of "digital innovation". This is another frequent issue, as whilst it is possible to outline the list of technologies that are novel and should have priority (e.g. big data, artificial intelligence) there are other technologies that cannot be considered novel but still are important for businesses and people yet simultaneously entail risk (e.g. city supervision systems, data bases of social services like the services of an operator of a postal service or telecom companies).

Typically, there are two approaches — limiting "sandboxes" to financial services, or providing a wider list of technologies that may be applicable for "sandboxes" in case of regulatory approval

(on the basis of discretionary powers). Historically and traditionally, the first approach is more applicable, but at the moment there are experiments with digital innovations in other areas (e.g. transport, medicine).

On the one hand, the COVID-19 pandemic may lead to the development of both digital innovation and "sandboxes", as within the pandemic, digital technologies are becoming increasingly important in new areas of social life, the economy, the state, and municipal administration (Efremov & Yuzhakov, 2020). The experimental nature of their introduction in new areas should be guaranteed by (within reason) clear and flexible legislation.

On the other hand, there are doubts about the effectiveness of flexible norms for balancing public interests and business strategies (Zezsche et al., 2017).

The Russian approach is not typical, and may be helpful for other jurisdictions. However, in order to estimate the actual effectiveness of the regulation and practical results, we need to wait at least a couple of years after the enforcement of the law and "sandboxes" in practice.

The Russian Federation has no special law on "regulatory sandboxes" at the moment. Instead, there are two approaches towards legal experiments (not only in digital area).

The first approach entails accepting special regulation on various issues.

There are three recent examples of special laws — the Federal Law on the experiment to establish a special regulation in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in Moscow[12]; the experiment in taxation for a special category of taxpayers ("professional income tax")[13]; the experiment of the use of electronic documents in employment relationship management[14].

Another option is to establish the experimental regulation by an Act of Government, if the legislation does not prohibit it. This option was used for experiments with labeling of certain categories of goods (perfume and toilet waters, footwear, clothes, tobacco products, etc.) with means of identification (by individual 2-D code for each item). Prior to the implementation of mandatory labelling in each category, under the decision of the Government, experiments were conducted for interested governmental, non-governmental, and business participants. There are a number of initiatives for experiments in different areas on the basis of bylaws.

The second approach is actively launching "sandboxes". Following in the footsteps of British colleagues, in 2018 the Central Bank of the Russian Federation (subsequently — the Bank of Russia), within the framework of the implementation of the Basic Guidelines for Financial Technologies Development for the period 2018-2020, launched its own "sandboxes"[15].

---

[12] Federal'nyy zakon № 123-FZ «O provedenii eksperimenta po ustanovleniyu spetsial'nogo regulirovaniya v tselyakh sozdaniya neobkhodimykh usloviy dlya razrabotki i vnedreniya tekhnologiy is-kusstvennogo intellekta v sub»yekte Rossiyskoy Federatsii — gorode federal'nogo znacheniya Moskve i vnesenii izmeneniy v stat'i 6 i 10 Federal'nogo zakona "O personal'nykh dannykh"» [Federal Law No. 123-FZ "On conducting an experiment to establish a special regulation to create the necessary conditions for the development and implementation of artificial intelligence technology in the subject of the Russian Federation — the city of federal significance in Moscow and amending Articles 6 and 10 of the Federal Law" On Personal Data"] (2020).

[13] Federal'nyy zakon № 422-FZ «O provedenii eksperimenta po ustanovleniyu spetsi¬al'nogo nalogovogo rezhima "Nalog na professional'nyy dokhod"» [Federal Law No. 422-FZ "On conducting an experiment to establish a special tax regime "Tax on professional income"] (2018).

[14] Federal'nyy zakon № 122-FZ «O provedenii eksperimenta po ispol'zovaniyu elektronnykh dokumentov, svyazannykh s rabotoy» [Federal Law No. 122-FZ "On conducting an experiment in the use of electronic documents related to work"] (2020).

[15] Bank of Russia. (n.d.). Regulyativnaya «pesochnitsa» [Regulatory "sandbox"]. https://www.cbr.ru/fintech/regulatory_sandbox/

This mechanism provides an opportunity to pilot innovative financial technologies and services on the financial market. Priority areas for piloting, according to the Bank of Russia policy, are Big Data and machine learning technologies, mobile technologies, artificial intelligence, biometric technologies, distributed registry technologies, open interfaces, digital profile technologies, and others. Any organization that has developed or plans to use an innovative financial service or technology can initiate piloting in a "sandbox".

The main problem of this initiative is the absence of any legal background, which leads to limited opportunities of potential participants. In fact, a participant's most fruitful opportunity is to create a model of whichever process they prioritize, and to convince the regulator that it is safe and not risky from the perspective of protecting important public values. The regulator is able to initiate changes in legislation, but this process takes much time. This type of "sandbox" is not flexible and risky, since the opportunity of launching "live" experiments is not available.

Unfortunately, the Bank of Russia does not post official information about the number of applications, decisions on them, and results of proposed "sandboxes". However, in February 2019, the Bank of Russia announced that the first project from the "sandbox" received legal approval. According to their official website, work on the project, which deals with the service that allows remote management of corporate client accounts for transactions in bank branches, began at least in August 2018. Sberbank (the largest bank in Russia, Central and Eastern Europe) was the initiator of this project. The testing was conducted jointly with professional associations of financial market participants and relevant government agencies. The Bank of Russia, as well as experts, found it expedient to launch the service taking into account recommendations provided by the regulator[16].

This case demonstrates the potential mechanism, but there are at least two specific details. First, there was not any testing in real life, but only modeling by experts and agencies, so there remain potential risks in real life conditions that cannot be forecasted within the model. Second, the Bank of Russia found the service does not require amendments to legislation — it was legalized by a bylaw.

According to mass media there are about 20 applications for the Bank of Russia's "sandbox", but the official statistics is not available.

This "theoretical" option is only for banks and other financial institutions that are supervised by the Bank of Russia. The same option is not available for other companies and other services.

Within the framework of the Digital Economy National Program[17], the Government of the Russian Federation mandated the Ministry of Economic Development to establish "legislative regulation of the creation and functioning of special legal regimes in the digital economy ("regulatory sandboxes")" by the end of July 2019.

With the short delay, in March 2020, Russian Ministry of Economic Development prepared a draft, agreed upon by all relevant federal executive agencies, of the Federal Law "On experimental legal regimes in the area of digital innovations in the Russian Federation"[18]; now this has been proposed by the Government to the State Duma, it may finally be approved by the end of the year.

[16] Sberbank. (2018, August 17). *Sberbank's service is first to pass piloting of Bank of Russia's regulatory sandbox*. https://www.banki.ru/ news/lenta/?id=10619991

[17] The Digital Economy National Program is aimed at creating a safe and powerful infrastructure for high-speed data transfer, processing, and storage, which will be made available for all organizations and households of Russia. One of the focus areas of the project is developing an up-to-date legal regulation, which involves creating favorable competitive conditions for the participants of the digital environment and introducing uniform requirements for electronic operations (Hohlov & Ershova, 2019).

[18] The draft of the Federal Law is available in Russian on the official website of the State Duma of the Federal Assembly of the Russian Federation. https://sozd.duma.gov.ru/bill/922869-7

However, the draft requires a satellite law with the details in relevant legislation (18 laws that should be amended are in the list of the Government), but this draft has not been prepared on time due to arguments within the federal agencies.

The key idea of the suggested regulation is pretty close to typical models considered above, and is under development within the experimental area, through which it will be able to do what is not quite allowed yet. If the experiment is successful, this regime will become the prototype of the new regulation across assorted areas of using digital innovation.

According to the draft, "regulatory sandboxes" will work in eight areas:

1) medical practice, including telemedicine technologies, technologies for the collection and processing of information on citizens' health and diagnoses, pharmaceutical practice;
2) design, manufacture, and operation of vehicles, including highly automated vehicles and unmanned aerial vehicles, certification of their operators, provision of transportation and logistics services, and the organization of transportation services;
3) e-learning and distance learning technologies;
4) financial markets;
5) remote sale of goods, works, and services;
6) architectural engineering, construction, major repair, reconstruction, demolition of capital construction objects, operation of buildings and structures;
7) state and municipal services providing and executing state control and municipal control;
8) industry.

The legal experiment is supposed to be extended to systems based on digital innovations, including Big Data, blockchain, neurotechnology and artificial intelligence, quantum technologies, robotics, etc. However, the draft does not have the list of technologies — it uses the term "digital innovation" in its broader meaning (a new or highly improved product).

In order to legalize special bylaw norms that overrule legislation for "sandboxes", the draft operates with two notions — general regulation (for all entities) and special regulation (for the participants of a "sandbox" for the limited period of an experiment).

Surprisingly, the list of participants consists of not only legal entities and entrepreneurs, but also of governmental (federal and regional) bodies, municipal bodies (for monitoring and oversight activities), and state and municipal services. This provision seems illogical, as in this area the state is able to make such legislation flexible.

The key idea of the draft is to create a procedure for developing the special (experimental) regulation of up to three years for participants in using different digital innovation and connected processes.

As oppose to the Republic of Kazakhstan, where the special regulation works only within the Astana International Financial Center[19], the Russian legislator does not draw the limits for territory[20] — "sandboxes" may work within the municipality, the region, or nationwide.

---

[19] According to the Constitutional Law of the Republic of Kazakhstan of December 7, 2015 No. 438-V "On International Financial Center Astana" (as amended and supplemented as of 30.12.2019), the hierarchy of norms within the Centre consists of three levels — the present Constitutional Law; acts of the Centre that are not contradicting the Constitutional Law, which may be based on the principles, norms, and precedents of the law of England and Wales and (or) standards of the leading world financial centers, accepted by the Centre's bodies within the limits of powers provided by the present Constitutional Law; and the current legislation of the Republic of Kazakhstan, which is applied in the part not regulated by this Constitutional Law and Acts of the Centre.

[20] There is a special regulation of the Innovation Centre "Skolkovo", but this example is unique. See: Federal'nyy zakon № 2 44-FZ «Ob innovatsionnom tsentre "Skolkovo"» [Federal Law No. 244-FZ "On Innovation Centre "Skolkovo"] (2010).

The draft creates a procedural mechanism for setting up, changing, cancelling, and monitoring "sandboxes". Under this mechanism, upon the application of an initiator or the request of the regulator (e.g. the Ministry of Digital Development, Communications and Mass Media of the Russian Federation for telecommunication or postal services), the government and business community organizations will be able to estimate the initiative and suggestions for the special regulation, and decide whether this regulation may be settled.

The initiator should provide the draft of the "sandbox" Program complete with an analysis of the risks, specific regulatory problems, and gaps that are considered to be boundaries for the implementation of the digital innovation with no special regulation.

The final decision on the application or request is made by the Government of the Russian Federation (of the Bank of Russia for its area of regulation) after the approval of two federal executive bodies (the regulator and "the designed in experimental legal regime" body) and a business community organization in the area of the experiment.

The procedural mechanism is clear and pretty democratic: it offers the opportunity to settle disputes and other disagreements, but the grounds of these decisions, as well as the authorities, are not transparent.

It is not obvious whether a business community organization is the only organization for all "sandboxes" or not; the criteria for this organization are not mentioned, and nor is the procedure of nominating whichever organization is chosen.

As the draft of the law declares, "sandboxes" will make it possible to check how a new technological solution works in real life within the special regulation, as well as to determine whether its universal use is acceptable and what requirements should be set when implementing it. The experiment includes assorted specific exemptions from mandatory requirements or special requirements for the participants of the "sandbox", in cases where there is a gap in regulation. The experiment may require the special incurrence of liability, but it is not mandatory. These exemptions, however, must not limit the level of protection of the rights and freedoms of citizens, state security, and other important constitutional values.

Reduction of terms helps to both reduce costs and replicate new solutions. Moreover, it allows quickly sifting out failing business models.

According to the results of the experiment, the new regulation of innovation areas is formed by the regulatory bodies if the "sandbox" is successful.

However, the detailed prescriptions about the requirements to these special regulations are going to be determined in relevant legislation (e.g. medical law for telemedicine services; transport law for drone taxis).

The advantage of suggested regulation is in the creation of the unified universal mechanism for "sandboxes" in all areas, and in detailed procedures with limited terms, authorities, and methods of decisions for each stage of approval. Moreover, this system is flexible enough, and not limited to financial services.

Meanwhile, the suggested mechanism has disadvantages and weaknesses that should be considered.

There is also a theoretical issue — how to protect public order if the executive bodies are able to postpone (or even cancel) laws for the list of entities. The rule of law guarantees that legislation cannot be overruled by bylaws. However, it is important to remember the concept of "delegated legislation"[21] — this theoretical challenge may be easily solved by special law on "sandboxes".

[21] With regional specific, this notion may be defined as the mechanism of delegation by the parliamentary authorities to executive bodies on the basis of legal provisions and within the framework of these provisions.

There are also practical issues that are important in the draft of federal law; three of these are the most urgent for consideration:

1) Firstly, the proposed mechanism contains multiple corruption risks at all stages, as there are no criteria for decision-making. All discretionary powers have no limits and/or adequate criteria for any decisions they may make. In fact, this is not a big problem, but the absence of an effective and fast judicial review gives the authorities unlimited power for the purposes of the application processing. In theory the standard judicial mechanism is undoubtedly still available, but this may work only in cases of procedural major violations that are significant enough. However, the grounds of decisions are closed and their publication is not mandatory; this leads to no judicial review being conducted of them. Another point is the grounds for choosing the "business community organization", as designed for the purposes of "sandboxes" processing.

2) Secondly, there are risks of unfair components and restricted commercial data disclosure during the application processing. Almost each digital innovation deals with new business processes and ideas that should not be disclosed. Another point is about the potential conflicts of interests of competing companies, and the opportunity to protect corporative interests only. The same problem is possible for startups and small companies with no representation in "a business community organization". In practice (even with at least three bodies at the first stage), "sandbox" processing may be used as a way of competence at whichever market companies see as fit. The absence of a predictable level of protection of interests is a significant gap in the draft for initiators and their commercial data. According to the previous version of the draft of the law, the Federal Antimonopoly Service opinion was mandatory; this provision however was not included in the final governmental draft.

3) Thirdly, business models are connected with other regulatory factors like taxation, licensing, and similar fields. Changing of legislation that affects the "sandbox" leads to the cancellation of it, according to the provisions of the draft of the Federal Law. On the one hand, this refers to the sovereignty of parliament and the law as the highest level of regulation. On the other hand, if the law comes into force, parliament will give the "mandate" to the Government or the Bank of Russia to exempt regulation for the limited period of time and limited list of participants. The previous version of the draft has the provision that the tax burden for participants of sandboxes cannot grow during the experiment; the current draft does not have this provision.

However, it looks like the Government does not plan to take "sandboxes" into force soon. Neither a draft of satellite law is ready, nor have the plans for preparing the draft for the second hearing at the State Duma been announced.

There is an idea to hold an experiment on settling "sandboxes" before or alongside changing the regulation. On June 16 2020, it was announced that the Ministry of Economic Development prepared the list of the projects that they are going to test as "sandboxes"[22].

There are six initiatives in this list, including: the service to protect subscribers from fraudulent calls based on Big Data and machine learning (the main regulatory issue is in the special regime of call data); remote signing a cellular service agreement with no necessity to visit the office of the operator (there are regulatory gaps in the legislation on communication as well as counter-terrorism provisions); "smart hotels" with automatic check-in; cargo transportation with drones; autonomous driving system with drones (with no engineers operating the system); medical care services through telemedicine (there is a provision that requires the first offline doctor's appointment).

[22] Vinogradova, E. (2020, June 16). Eksperimental'no, Vatson: Minek uzakonit antifrod-servisy v «pesochnitsakh» [Experimentally, Watson: Ministry of Economic Development will legitimize antifraud services in "sandboxes"]. Izvestia. https://iz.ru/1023765/ekaterina-vinogradova/eksperimentalno-vatson-minek-uzakonit-antifrod-servisy-v-pesochnitcakh

On June 16 2020, the draft of satellite law was published for the purposes of independent anti-corruption expertise[23], but it is not final draft.

Unfortunately, the draft provides tailored solutions as it consists of the closed list of mandatory and other requirements that may be limited, cancelled, or modified within a "sandbox". This draft includes pretty brief regulations with amendments to 8 laws (in the areas mentioned above)[24] with the lists of articles and provisions "which apply unless otherwise provided" by a "sandbox".

The analyzed Russian approaches are illustrative and may be helpful for other jurisdictions, especially for developing countries that do not have the analogue experience.

The idea of "sandboxes" has already been added to by the new direction of regulatory development, which may be considered as "smart regulation" (Hohlov & Ershova, 2019), but these concepts are not competing — both of these institutions may be used simultaneously.

Moreover, if the regulation is rigid and not flexible enough (as is pretty typical for most post-Soviet countries, as well as a number of developing countries), "sandboxes" will help to improve legislation after testing all processes and requirements in real-life circumstances to facilitate the intensive and effective development of digital technologies and innovations.

The provisions of the suggested regulation may be changed dramatically during hearings in the Federal Assembly of the Russian Federation, but it is best to hope that the key ideas and approaches will be included in the law.

Time will tell how effective and appropriate this universal mechanism of "sandboxes" is to the reality of life and law in Russia.

[23] The draft available in Russian at the official web-site: https://regulation.gov.ru/projects#npa=102951

[24] Before, the Government of the Russian Federation outlined 18 federal laws to be amended.

References:

1. Allen, H. (2019). Regulatory sandboxes. *George Washington Law Review, 87*(3), 579–645. https://digitalcommons.wcl.american.edu/facsch_lawrev/709
2. Bromberg, L., Godwin, A., & Ramsay, I. (2017). Fintech sandboxes: Achieving a balance between regulation and innovation. *Journal of Banking and Finance Law and Practice, 28*(4), 314–336.
3. Efremov, A., & Yuzhakov, V. (2020). Experiments in the field of digital technologies under conditions of pandemic: potential, current state and problems [Experimenty v sfere tsyfrovykh tekhnolofiy v usloviyakh pandemii: potentsial, tekuschee sostoyanie i problimy]. *Monitoring of the Economic Situation in Russia: Trends and Challenges of Social and Economic Development, 115*(13), 31–38.
4. Fenwick, M., Wulf, A., & Vermeulen, E. (2017). Regulation tomorrow: What happens when technology is faster than the law? *American University Business Law Review, 6*(3), 561–594. https://doi.org/10.2139/ssrn.2834531
5. Hohlov, Yu., & Ershova, T. (2019). Russian digital economy program. *IAC Online Journal CIO and Digital Innovation, 2*(1), 35–38.
6. Huang, R., Yang, D., & Loo, F. (2020). The Development and regulation of cryptoassets: Hong Kong experiences and a comparative analysis. *European Business Organization Law Review, 21,* 319–347. http://dx.doi.org/10.2139/ssrn.3544034
7. Wechsler, M., Perlman, L., & Gurung, N. (2018). *The State of regulatory sandboxes in developing countries.* Columbia Institute for Tele-Information. http://dx.doi.org/10.2139/ssrn.3285938
8. Zetzsche, D., Buckley, R., Arner, D., & Barberis, J. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *European Banking Institute Working Paper Series, 23*(1), 31–103. http://dx.doi.org/10.2139/ssrn.3018534

Information about the author:

Damir R. Salikhov — Ph.D. in Law, Teaching Assistant of the Chair of Constitutional and Municipal Law of Lomonosov Moscow State University, Faculty of law, Moscow, Russia.
d_salihov@law.msu.ru

Сведения об авторе:

Салихов Д.Р. — кандидат юридических наук, ассистент кафедры конституционного и муниципального права Юридического факультета Московского государственного университета имени М.В. Ломоносова, Москва, Россия.
d_salihov@law.msu.ru

https://doi.org/10.38044/2686-9136-2020-1-2-28-40

JEL: K10, O43, P26

ARTICLES

YELLOW BRICK ROAD TO DIGITAL STATE

Vladimir S. Osipov

Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

Abstract

The subject of the research is the transformation of the state institution under the influence of the digital revolution. The choice of topic is determined by the transition of the state institution from bureaucratic to service and from service to digital. This transition entails significant changes in the methods of regulating public relations, the forms of state participation in the life of citizens, as well as the architecture of interaction between state, business and society in the new environment. The aim of the research is to create and justify a model of digital public administration, in which the necessary access to personal information of the digitized state will not be used against citizens. Therefore, the digitalization of public administration should be a tool to improve the efficiency of public services. The research methods are: institutional and comparative legal analysis, as well as methodology of value chain management by M. Porter. The results of the research show that (1) the created value chain of public administration includes main and auxiliary activities in the system of public administration in the digital state, (2) changes in the governance due to the increasing role of the digital state have been proved based on the doctrinal components of the new public administration of C. Hood, and (3) substantiated the reasons for the evolution of public administration through the prism of management structures: from linear-functional to project-functional structure and, as a result, to state digital platforms. Based on the declarations of the UN General Assembly, the conclusion is made that it is necessary to strengthen the control of the judiciary over the executive to avoid the establishment of digital totalitarianism. These findings reinforce the methodological significance of the evolution of public administration, as well as the practical value in reforming the system of governance under the influence of the digital revolution.

Keywords

digital state, public administration, value chain of public administration, human privacy, digital totalitarianism

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Osipov, V. S. (2020). Yellow brick road to digital state. *Digital Law Journal, 1*(2), 28–40. https://doi.org/10.38044/2686-9136-2020-1-2-28-40

Submitted: 06 Apr. 2020, accepted: 30 Jun. 2020, published: 20 Yul. 2020

СТАТЬИ

ДОРОГА ИЗ ЖЕЛТОГО КИРПИЧА К ЦИФРОВОМУ ГОСУДАРСТВУ

В.С. Осипов

Московский государственный институт международных отношений (университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

Аннотация

Предметом исследования в статье выступает трансформация института государства под влиянием цифровой революции. Выбор темы определяется переходом государственного учреждения от бюрократического к сервисному и от сервисного к цифровому. Этот переход влечет за собой значительные изменения в способах регулирования общественных отношений, формах участия государства в жизни граждан, а также в архитектуре взаимодействия государства, бизнеса и общества в новых условиях. Целью исследования является создание и обоснование модели цифрового государственного управления, в которой необходимый доступ к личной информации цифровизированного государства не будет использоваться против граждан. Поэтому цифровизация государственного управления должна стать инструментом повышения эффективности государственных услуг. Методы исследования: институциональный и сравнительно-правовой анализ, а также методология управления цепочкой ценности М. Портера. Результаты исследования показали, что (1) созданная цепочка ценности государственного управления включает основные и вспомогательные виды деятельности в системе цифрового государственного управления; (2) на основе доктринальных компонентов нового государственного управления Ч. Худа предложено соответствующее изменение в системе государственного управления в связи с возрастанием роли цифрового государства и (3) эволюция бюрократического, сервисного и цифрового государства, а также их аппаратов посредством структур управления происходит по следующему сценарию: от линейно-функциональной к проектно-функциональной структуре и к государственным цифровым платформам. На основании деклараций Генеральной Ассамблеи ООН сделан вывод о необходимости усиления контроля судебной власти над исполнительной во избежание установления цифрового тоталитаризма. Эти выводы подтверждают методологическую значимость эволюции государственного управления, а также практическую ценность реформирования системы государственного управления под влиянием цифровой революции.

Ключевые слова

цифровое государство, государственное управление, цепочка ценности государственного управления, права человека и гражданина, цифровой тоталитаризм

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Осипов, В. С. (2020). Дорога из желтого кирпича к цифровому государству. *Цифровое право, 1*(2), 28–40. https://doi.org/10.38044/2686-9136-2020-1-2-28-40

Поступила: 06.04.2020, принята в печать: 30.06.2020, опубликована: 20.07.2020

Introduction

States that transition from one political order to another do so with different aims. Their economic situation, sustainable power structures, the maturity of civil society, and their international competitiveness are factors that inform this transition. This last feature requires the creation of an effective institutional environment to attract investments, raising the quality of human capital and technological modernization.

A favorable environment for economic development has been created by the technologies of the 4th industrial revolution, the Internet of things, and the digitalization of an increasing number of processes for production and service. They help to increase efficiency after all other management tools have already been implemented and have exhausted their capabilities. When the public administration system is assessed, the problem of efficiency can clearly be found there too. The transition from a bureaucratic state to a service state was done with the aim of increasing how efficient public administration could be. This would transpire by reducing the cost of performing public functions, whilst also improving their quality by optimizing service times, reducing waiting times, using budget funds in a targeted way, and individualizing state support for citizens.

The idea itself turned out to be quite attractive; it was first adopted by the United Kingdom (Barber, 2008), and later by many other states, including Russia. Criticism, however, was leveled at this approach almost immediately; service standardization was introduced as part of the transition to a service state, raising new problems. It turned out that, since citizens differ vastly in their requirements, their needs do not fit into the approved standards for the provision of public services. The transition from a bureaucratic to a service state was reminiscent of the transition from artisanal production to mass production; however, it was business that realized the significant diversity of human needs, and thus the inefficiency of mass production. Due to the hyper-competitive struggle, business was forced to switch to mass customization, which could individualize and satisfy various consumer needs. The inconveniences that service states place on their citizens also exposed how dissatisfied they were with public services. Here, however, this problem resulted in a decrease in the level of trust citizens held in their state, which could be fraught with social upheavals. This outcome did not suit the authorities.

The transition of the political order from a service state to a more efficient system proved to be an urgent problem, yet a solution was found rather quickly, prompted yet again by business. For states that are rapidly losing their citizens' trust, digitalization has shown itself to be a lifeline. There has been a rapid growth in states which are transferring the order of their services to digital platforms. Estonia and Denmark were ahead of all other countries in the digitalization of their public administration.

In terms of the digitalization of the public services system, Estonia and Denmark are world leaders. In Estonia, almost all public services are provided digitally, apart from acts of civil status where a personal presence is necessary (marriage and divorce, as well as the purchase of real estate while making entries in the state cadastre). The authorities of both Denmark and Estonia were able to implement state digitalization projects; in terms of scale, these projects were comparable to the largest internet platforms (Fuchikawa, 2020). Importantly, the governments of countries leading in digitalization, as well as internet platforms, have set consumer needs as priorities, and agile technologies (flexible testing and learning methods) as their implementation method. The use of agile methods alone would not ensure success when digitalizing public services: changing the flow of information

is not consistent with consumer interests and, vice versa, the interests of consumers do not always coincide with the results of optimizing information flows.

At the same time, some state bodies cannot provide a unified architecture for their digital environment. In these situations, they are forced to coordinate their actions and projects at the governmental level (Osipov, 2016); when digitalizing their public service system, this acts as a consolidating and directing center. The role of each national government is not limited to consolidating the ideas of disparate and independent state bodies; the tasks faced by national government are much greater than might seem at first glance. The government should not only develop, approve and implement their digitalization strategy (in which the goals, objectives, priorities, and methods of its implementation are clearly fixed); it should also offer a unified IT platform, as well as the technical standards necessary for developing the components necessary to underpin their digital environment (with the possibility of their integration with each other based on a single digital platform), and ensure the timely submission of bills to parliament, which will fix new institutional conditions for the provision of public services amongst many others[1].

The transition from a service state to a digital one also has a number of requirements. The first consideration is the coverage and quality of internet connection. It is no coincidence that it was Estonia and Denmark that were among the leaders in constructing a digital state — for implementing such large-scale internet platform projects, a small territory and a small population turned out to be positive characteristics.

Both in terms of population and territory, Russia is much larger, which means that its task of digitalization is much more complicated. However, this is merely the technical side of the matter; cell towers, satellite launches, and fiber optic networks can solve the coverage problem. However, another, much more serious problem almost always casts a shadow over technological advances in public administration: respecting the right to privacy. In countries where either bureaucracy and/or the service state are the prevailing political ideologies, it has been relatively easy to balance efficient digitalization with non-interference in citizens' private lives. For such public administrations, it is relatively easy to adopt a system of internet platforms and digitalize public services.

Institutions streamline how citizens and organizations act and contribute to stabilizing the state. If, however, the state is the main institution (or institution of institutions), the different levels of institutions must be clarified; branches of Big Government include executive institutions, legislative institutions, and judicial institutions. The most important condition for state sustainability is the balance between these branches. Obviously, the violation of this balance ultimately leads to instability, social upheaval, and even revolution.

However, it must be not forgotten that, at the end of the 20th century, about forty countries transitioned from authoritarianism or totalitarianism regimes to democracy. As the USSR collapsed, and a number of former socialist states transitioned to democracy, this mass change of regime should, in theory, have bought the problems of state science to the forefront of theoretical and legal research in sciences, especially since this transformation affected 24 CMEA countries (including observers and associate members). Some CMEA member countries have split up into separate independent states — for example, the Socialist Federal Republic of Yugoslavia, the Czechoslovak Socialist Republic, the USSR, and the German Democratic Republic completely ceased to exist. Considering this, it seems

[1] Daub, M., Domeyer, A., Klier, J., & Lundqvist, M. (2017). *Digitizing the state: Five tasks for national governments*. McKinsey& Company. https://www.mckinsey.com/industries/public-sector/our-insights/digitizing-the-state-five-tasks-for-national-governments

more than strange that the crucial issue of rediscovering the laws of formation and disintegration of states was not discussed in legal sciences; these were driving forces behind these states' historical development. Among such regularities, so-called "path dependence" can be clearly traced, which assess how future developments depend on previously achieved results, national characteristics, habits, beliefs, etc.

It is interesting to imagine that, by virtue of digitalization, such states can receive total control over the individualized information of each citizen, despite their background of exerting a totalitarian political order. Due to the gauge effect, individual statesmen could seek to establish unlimited power using the received official information.

In connection to this, in his famous "History of the Government", S.E. Finer convincingly argues that, throughout the 5200 year historical trend he describes, "the longevity of the state is ensured by the well-developed institutional structure of the state and its ability to unity in action" (Finer, 1997). Thus, it is not only international competitiveness that is dependent on a well-developed institutional structure, but also the longevity of the state.

This is a transition (or departure) away from the Marxist-Leninist doctrine, where the state is an arm of the ruling class and reflects their political power; notoriously, Lenin noted that the state can be a special tool for exerting control. When the state had the grounds for keeping one part of society from another, the Marxist-Leninist philosophy predicted that, if the basic conditions for creating a classless society were fulfilled, "the socialist state may wither away"; Lenin's hope was for the onset of communism to instigate this withering. The utopian idea of a classless society, as well as the political transformation in almost forty countries (CMEA countries and the Republics of the former USSR), should have manifested itself in political studies into the process of how a political order transforms and the results of such a process. Furthermore, the result of the transformation process is reflected, as we see it, in the institutional structure of the state and its stability.

Following the previously expressed ideas, special institutions play a rather important role in the development of states, contributing to the formation and transition to the next stage of development.

We are critical of the economic category of "institution", and use it only as a term denoting institutions rather than norms and rules (although they remain in the theory of law). Our definition of the state follows that of Maurice Hauriou, the French lawyer who first conveyed the idea that the State — acting as the organizer, controller, and coordinator of social and political order — is the institution of institutions. Therefore, for us, regarding the political, economic and legal systems which society follows, the state is an institution of institutions, or the main institution above all (Hauriou, 1910).

Methodology

Institutional analysis and legal comparative analysis were used in the article to identify and justify the institutional structure of a state on its way to digitalization. An interdisciplinary approach was used in the research because institutional theory has a duality, based to both legal and economic sciences. Legal science laid the theoretical foundations of institutionalism, and economic science contributed to the implementation of the ideas of institutionalism in the practice of political order transition and public administration.

The necessity to move from a service state (with its mass standardized approach to satisfying citizens' needs) to a digital state (with mass individualized satisfaction of citizens' needs for public services) was brilliantly shown by Michael Porter in his famous figure of the value chain (Porter, 2004).

We have taken advantage of its development, and will show how the public administration system can be analyzed from the perspective of this value chain; the needs of the consumer must be met as and when it is convenient for them. We called this figure the Value Chain of Public Administration (Figure 1).

As can be seen in figure 1, public policy can conditionally be divided into two large groups of policies: main and support.

The main policies have conditional stages, as well as stages in the manufacture of a product in business: from incoming material, information, and financial types of flows (amongst others), through their transformation, into an outgoing flow. The marketing block comes afterwards. By thinking about what products we associate with individual countries, it becomes clear that each country, due to the international division of labor, specializes in its own product groups. Due to the transition to the VI technological structure, obviously, services occupy an increasing share of the structure of the economies of highly developed countries; therefore we distinguish services as the final level of the main policies of the state, which is something slightly separate. State policies which support this are diverse and specifically relate to each individual state, but we can distinguish these as: infrastructure, human capital development, technological development, and institutional policy.

Infrastructure is a block of supporting policies in the field of social development, industrial policy, transport, and the financial structure, but it is not limited to them.

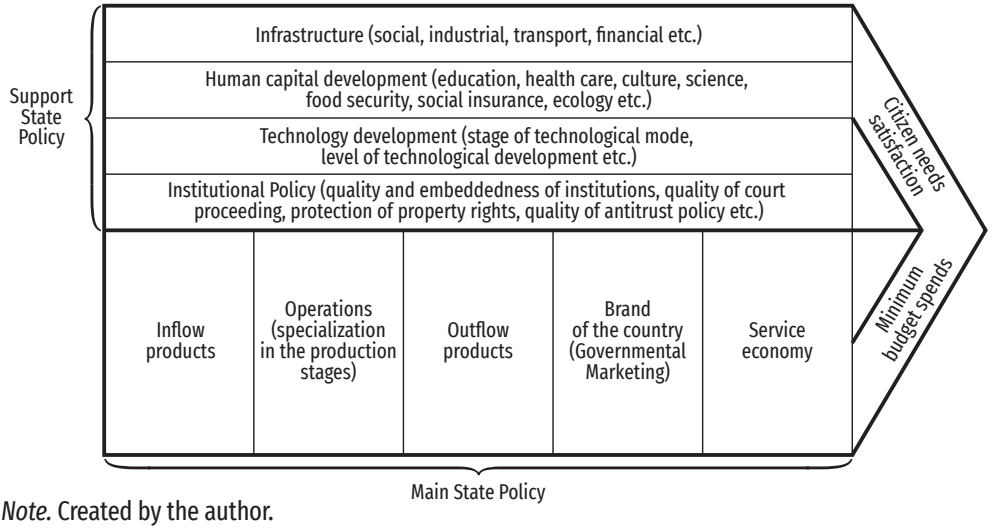
The development of human capital affects the areas of healthcare and medicine, education, culture, science, food safety, ecology, social insurance, etc.

Technology development stands out as a separate policy group, since it relies on the state at whichever stage of technological development it is; that is, it is reliant on how effectively the business is heading towards technological modernization.

Institutional policy forms the basis of all other policies. It consists of the quality and integration of effective market and state institutions that are aimed at the quality protection of property rights, quality justice, and protecting competition. This is the only part of the Value Chain of Public

Figure 1

Value Chain of Public Administration, Doctrinal Components of Modern Public Administration



Note. Created by the author.

Administration that the state can use in a coordinating role. The most important function here is to ensure fairness, without violating human and civil rights, when making decisions about security, protection, and law and order. The main institution here should be a court, which must be independent from the executive and legislative branches.

At the right end of the value chain, it can be seen that most politicians aim for a minimum of budget expenditures; this is the target performance indicator they aim to meet precisely. At the same time, supportive politicians aim to meet citizens' public service needs. It is here that a citizen faces the state face to face.

The unique, combinatory nature of the main and supporting policies — their quality, their interaction and their coordination — are a condition for a state's stable institutional structure as it transitions from one political order to another. In this case — in the transition from a service state to a digital one — the most important role is played by institutional policy, since all other policies seem to retain their essence in this transition. We take this methodology to describe the transition process of the state from a bureaucratic to a service and to a digital one.

Almost all the types of policies included in the Value Chain of Public Administration can be digitalized; due to new technologies, both the efficiency of spending budget funds and the quality of public administration services can be improved. The only policy which largely cannot be digitalized is institutional policy, since this is a mechanism on which the architecture of the entire public administration system of a digitalized state can be founded. The sustainability of the state depends on how effectively this function is realized and how sustainable the institutional structure is. For a digital state, this is also true, since satisfying the needs of public service consumers is not reliant on if the quality of these services is low and if citizens express their dissatisfaction through social upheavals that shock the state. Thus, institutional policy is the main component of state policy for maintaining the state's sustainability and development.

The philosophy of transitioning from a service to a digital state is based on satisfying the needs of the consumer, which is expressed precisely as a tool of the value chain.

Discussions

Public and private managements have long been interacting with each other (Lepawsky, 1949; George, 1972; Bourdieu, 2012; Mann, 2012). The business analogy and the methodology of professional economics revealed their influences on public administration. Public administration on all levels must be made cost-conscious — and hence efficient — by measuring the productivity of their services at whatever level they originate. It was argued that only by this macro means, in which the country was again made fully competitive, can the state hold its competitive global position (Dimock et al., 1983).

When Hood (1991) formulated his principles for new public management, he focused on the business practices and management tools of a business enterprise. As it happens, his ideas turned out to be revolutionary precisely because of how business practice transferred to the sphere of public administration. Paying tribute to Hood's ideas, we note that they remain relevant when reviewing the transition from a bureaucratic state to a service one**,** nor from a service state to a digital one.

Firstly, Hood correctly noted that, if a state maintained a long peaceful condition after the Second World War, they created for themselves a set of unique social prerequisites and economic conditions which contribute to the growth of the global economy. Indeed, a lasting peace creates opportunities for long-term forecasting, and thus public administration systems can be designed on an increas-

ingly effective basis. In wartime, this is completely impossible, since the logic of public administration is subordinated to a mobilization economy, as Andrain correctly notes (Andrain, 1994)

Sustainable economic growth created the conditions for a positive change in the levels of income and distribution mechanisms. Revolutionary technological changes have also had a significant impact on the socio-economic system, which has led to the removal of traditional barriers between "public sector work" and "private sector work" (Jessop, 1988). The work of state apparatus has become more and more like how corporations function: similarities can be seen in management tools, decision-making mechanisms, methods of selecting personnel, their promotion along the career ladder, etc.

The use of business tools in government — which are significantly different from bureaucratic tools — has led to a uniform approach to business and government.

This trend could not but lead to the digitalization of the state. The digitalization of business, and the creation of internet platforms and ecosystems, had already been rapidly developed. The state simply had to follow.

Swan noticed that one implication of blockchain governance is that the model of government could shift from being the compulsory, one-size-fits-all, "greater good" model — as it is at present — to one

Table 1

Doctrinal Components of New Public Management with Specific for Digital State

No.	Doctrine	Meaning	Typical justification	Specific for a Digital State
1	*'Hands-on professional management'* in the public sector	Active, visible, discretionary control of organizations from named persons at the top, 'free to manage'	Accountability requires clear assignment of responsibility for action, not diffusion of power	Responsibility for creating an internet platform in the form of value chain of public administration
2	*Explicit standards and measures of performance*	Definition of goals, targets, indicators of success, preferably expressed in quantitative terms, especially for professional services	Accountability requires clear statement of goals; efficiency requires 'hard look' at objectives	Transition from the mass satisfaction of citizens' needs to mass customized individualized satisfaction of citizens in public services
3	Greater emphasis on *output controls*	Resource allocation and rewards linked to measured performance; breakup of centralized bureaucracy-wide personnel management	Need to stress *results* rather than *procedures*	This task remains, since the project approach to solving public administration problems is not removed from the agenda when moving to a digital state

Continuation of Table 1

No.	Doctrine	Meaning	Typical justification	Specific for a Digital State
4	Shift to *disaggregation* of units in the public sector	Break up of formerly 'monolithic' units, unbundling of U-form management systems into corporatized units around products, operating on decentralized 'one-line' budgets and dealing with one another on an 'arm's length' basis	Need to create 'manageable' units, separate *provision* and *production* interests, gain efficiency advantages of use of contract or franchise arrangements *inside* as well as outside the public sector	Creation of a system of distributed solutions of public administration problems in public project offices
5	Shift to greater *competition* in public sector	Move to term contracts and public tendering procedures	*Rivalry* as the key to lower costs and better standards	Increased competition between state and business for IT professionals capable of creating and managing internet platforms
6	*Stress on private sector styles of management practice*	Move away from military-style 'public service ethic', greater flexibility in hiring and rewards; greater use of PR techniques	Need to use 'proven' private sector management tools in the public sector	Strengthening the trend towards the adoption of business tools regarding the creation of internet platforms and digital technologies from business to public administration
7	Stress on greater *discipline* and *parsimony* in resource use	Cutting direct costs, raising labour discipline, resisting union demands, limiting 'compliance costs' to business	Need to check resource demands of public sector and 'do more with less'	The trend continues and intensifies with the transition to a Digital State

*Note***.** Created on the base of Hood (1991).

that can be tailored to the needs of individuals; it is thus possible to imagine a world of governance services which is as individualized as Starbucks coffee orders. As an example of personalized governance services, one resident might pay for a higher-tier waste removal service that includes composting, whereas their neighbor pays for a better school package. Personalization in government services, instead of the current one-size-fits-all paradigm, could be orchestrated and delivered via blockchain (Swan, 2015). As can be seen, blockchain — as one digital technology — may be used in public administration videlicet for individualized needs in the satisfaction of citizens in public services.

The logic of state transformation and its apparatus is laid out in the following figure.

As history shows, the process of transforming from a bureaucratic state to a digital state requires going through a service state type. Due to this, it must be observed that transitioning directly from a bureaucratic state to a digital state is impossible, as states cannot jump from single production directly into mass individualized customization. This is a kind of law of the evolution in business and public administration. In this paradigm of transforming into a digital state, it is necessary to note the risks of violation of human rights.

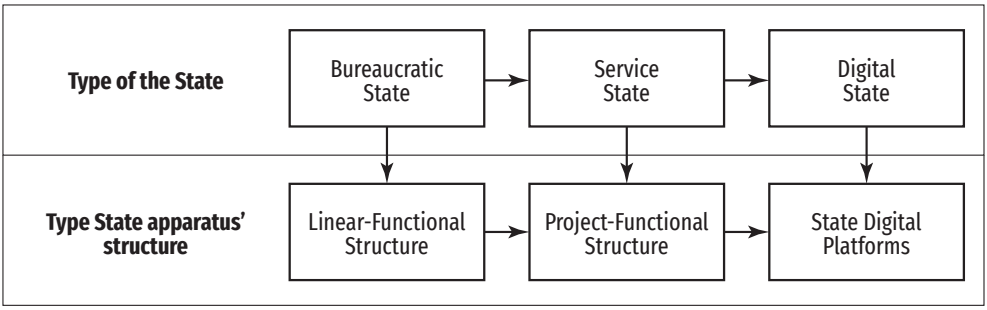
As law is digitalized, the risks of a technocratic attitude towards individuals increase; a person, their basic human rights and freedoms, and their security and dignity may be more susceptible to this threat. Berman noted that people mainly see the law as a mass of legislative, administrative, and judicial rules that apply in their country (Berman, 1994). Digitalization runs the risk of taking a further step towards the mechanization of law coming true. Primarily, the robotization and algorithmization of law enforcement are the main contemporary trend (Hong & Goodnight, 2020; Eldem, 2020).

Robotization is a specific technocratic paradigm which, in a developed and politically organized society, transmutes the law into a tool of social engineering and a highly specialized form of social control.

Pound noted that, under these conditions, "law" was given a new meaning. Conditions for this change include: social control as state control; the state as an end in itself; the legal order as a regime for ordering all conduct and dictating all adjustment of relations by official application of the force of a politically organized society to the case at hand; law as what those officials do because they do it; the judicial process as simply effective exertion of the power of the state officials (in other words, an omnicompetent state, in contrast with politically organized society carrying on a regime

Figure 2

Evolution of Types of the State and its Apparatus' Structure



Note. Created by the author.

of social control through orderly application of force according to prescribed models or patterns of decision and determination); a law state (Pound, 2002).

Facial recognition systems provide a very useful digital technology, which can make public services individualized, as has been noticed by Swan (2015). This technology is already used in banks for financial services, where offices no longer require documents to prove identify before providing financial services. Another way facial recognition systems are used is by the police and Interpol; the Interpol Face Recognition System (IFRS) contains facial images received from more than 160 countries, making it a unique global criminal database. As Interpol's official site makes clear (www.interpol.int), computerized facial recognition is a relatively new technology which law enforcement agencies around the world are introducing in order to identify persons of interest. Coupled with an automated biometric software application, this system is capable of identifying or verifying a person by comparing and analyzing the patterns, shapes and proportions of their facial features and contours. Proving its effectiveness, more than 650 criminals, fugitives, persons of interest, or missing persons have been identified since the launch of Interpol's facial recognition system at the end of 2016.

Of course, facial recognition systems allow wanted criminals to be identified; however, people who have committed no crimes or offenses, but whose movements will be controlled in order to track criminals, should be allowed to voice their opinion. Such controls could lead to the development of secrets in a citizen's personal life. There are people who take pleasure in showing themselves to the whole community, but not everyone shares this feeling. Knowing that they are being constantly monitored, does this not pose a threat to a citizen's mental health, as was notoriously noted by George Orwell (1945)?

Conclusion

The resolution adopted by the General Assembly on 18 December 2013 (on the report of the Third-Committee (A/68/456/Add.2)). 68/167 "The right to privacy in the digital age", reaffirms the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, as well as reaffirming the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. Following on from that point, the General Assembly notes that the problem of human rights in the digital age is in the full growth, with no reasons to say that almost 7 years the situation is becoming better; the General Assembly also affirmed that the same rights that people have offline must also be protected online, including the right to privacy. In this case it must be noted that this point runs counter to the task of security and facial recognition systems, and also with free access of state security bodies to mobile calls, SMS, and suchlike. In addition, the access internet platforms have to the private lives of citizens must be assessed. Internet platforms track user requests and offer contextual advertising, information, or products in accordance with user requests. As mentioned above, the General Assembly's Resolution warns of threats to privacy, and names the tasks the state must undertake to respect and protect the right to privacy, including in the context of digital communication. It also suggests measures that must be implemented to put an end to any violations of those rights, and the conditions that must be created to prevent such violations, including by ensuring that relevant national legislation complies with obligations under international human rights law. Using digital platforms to collect personal data runs counter to personal privacy.

The resolution adopted by the General Assembly on 18 December 2013 (on the report of the Third-Committee (A/68/456/Add.2)). 68/168 "Globalization and its impact on the full enjoyment of all human rights" recognizes that while globalization may affect human rights (by its impact on, inter alia, the role of the State), the promotion and protection of all human rights is first and foremost the responsibility of the State. Protecting human rights holistically is a task for individual actors/States, who have their own goals of security, and thus may be interested in violating human rights — for altruistic reasons — to achieve such security. However, if the State predicts threats against its power, such data can also be collected and used against individuals. Looking to the future, there is conflict of interest between the responsibility of Digital State to protect privacy as basic human right, and the task of Digital State to control people and their political activity.

This conflict of interest is the key problem Digital States face at present and in the foreseeable future. If this problem is not solved, people around the world will face a new digital totalitarianism; if so, supposed democracies could exert total control over the behavior of their citizens.

The essentials of digital totalitarianism include the extinction of the spirit of justice, the removal of emotional sources of thoughts, formal logical solutions to disputes, and the denial of the *spirit* of the law in favor of its *letter*. The problem is that all citizens are different from each other, but in the framework of algorithmization, these differences in nature cease to exist and each citizen becomes just a registration object with serial number. Commonly, this political order is called "digital totalitarianism", as there are many similarities between this public administration and the worst examples from history.

Strengthening the role of the Constitutional court could solve this problem; this is the solution we propose. By virtue of its authority, the court should work more diligently to verify that executive authorities, if they try to establish control over the society using digital technologies, comply with fundamental human rights. Such a decision is possible only if the constitutional court is truly independent from the executive authorities, which today seems utopian. It would be necessary to strengthen the role of legislative power in the formation of the constitutional court, and to protect the judges of the constitutional court from pressure from the executive authorities. The power balance of legislative and executive bodies in the formation of a constitutional court can lead to the judiciary as a whole exerting increased independence; to us, this seems the only way to avoid slipping into digital totalitarianism.

References:

1. Andrain, C. F. (1994). *Comparative political systems. Policy performance and social change*. M.E. Sharp. https://doi.org/10.5860/choice.32-2358
2. Barber, M. (2008). *Instruction to deliver. Fighting to transform Britain's public services*. Methuen Pub. Ltd.
3. Berman, H. J. (1983). *Law and revolution. The formation of the western legal tradition*. Harvard University Press.
4. Bourdieu, P. (2012). On the state [Sur l'Etat]. Le /Seuil et Raisons d'Agir.
5. Dimock, M. E., Dimock, G. O., & Fox, D. M. (1983). *Public administration*. (5th ed.). Holt, Rinehart and Winston.
6. Eldem, T. (2020). The governance of Turkey's cyberspace: between cyber security and information security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689
7. Finer, S. E. (1997). *The history of government.* (Vols. 1-3). Oxford University Press.

8. Fuchikawa, K. (2020). Regulations of digital platform markets under the Japanese Antimonopoly Act: Does the regulation of unfair trade practices solve the Gordian knot of digital markets? *Antitrust Bulletin*, *65*(1), 102–119. https://doi.org/10.1177/0003603X19898905
9. George, C. S. Jr. (1972). *The History of Management Thought*. Prentice-Hall.
10. Hauriou, M. (1910). Principles of public law [Principes du droit public]. Larose et Tenin.
11. Hong, Y. & Goodnight, G. T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication*, *13*(1), 8–26. https://doi.org/10.1080/17544750.2019.1687536
12. Hood, C. (1991). Public management for all seasons? *Public Administration*, *69*, 3-19. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x
13. Jessop, B. (1988). Conservative regimes and the transition to post-fordism: The cases of Great Britain and West Germany. In M. Gottdiener & N. Komninos (Eds.), *Capitalist development and crisis theory: Accumulation, regulation and spatial restructuring* (pp. 261-299). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-19960-0_11
14. Lepawsky, A. (1949). *Administration: The art and science of organization and management*. Knopf.
15. Mann, M. (2012). *The Sources of Social Power*. (Vol.2; 2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139381314
16. Orwell, G. (1949). *Nineteen Eighty-Four*. Secker and Warburg.
17. Osipov, V. S. (2016). Proektno-funktsionalnaya struktura upravleniya dlya gosudarstvennykh organov [Project-Functional Structure of Management for Public Administration]. *Public Administration Issues,* (3), 219–230.
18. Porter, M. E. (2004). *Competitive advantage. Creating and sustaining superior performance*. Free Press.
19. Pound, R. (2002). *The ideal element in law*. Liberty Fund.
20. Swan, M. (2015). *Blockchain. Blueprint for a new economy*. O'Reilly.

Information about the author:

Vladimir S. Osipov — Dr. Sci. in Economics, Ph.D. in Economics, Associate Professor, Asset Management Department, Moscow State Institute of International Relations (MGIMO-University), Moscow, Russia.
vs.ossipov@inno.mgimo.ru

Сведения об авторе:

Осипов В.С. — доктор экономических наук, Ph.D., доцент, профессор кафедры управления активами Московского государственного института международных отношений (университет) МИД России, Москва, Россия.
vs.ossipov@inno.mgimo.ru

https://doi.org/10.38044/2686-9136-2020-1-2-41-52

ARTICLES

PRIVATE LIFE AND SURVEILLANCE IN A DIGITAL ERA: HUMAN RIGHTS IN EUROPEAN PERSPECTIVE

Roman V. Prudentov

Freshfields Bruckhaus Deringer LLP
65, Fleet str., London, UK, EC4Y 1HS

Abstract

This paper focuses on identifying key legal considerations and developments in the area of surveillance in Europe in human rights, with its emphasis on the jurisprudence of the European Court of Human Rights. The aim of this research was to enhance and align law and practices in this area in Russia and Europe. The author analysed the core and most novel Court cases that may be applicable to the subject matter, including by analogy, as well as the latest research in this area. This paper considers, *inter alia*, ability to challenge relevant law and practices *in abstracto*, legitimate aims justifying interference, the requirements for the relevant laws, fetters to authorities' discretion on surveillance matters, and appropriate nature of supervision by authorities and the scope of their powers, as well as certain other safeguards. This paper also discusses interactions and balances between freedom and security, modern approaches taken by the EU and the US, and tensions on pervasive surveillance matters. This paper reveals that, in a COVID-19 world, with those privacy issues that arise from the "track and trace" system and similar practices having already been widely scrutinised by the courts, it is possible to fight COVID-19 through surveillance methods with minimum interference with human rights. Key considerations outlined in this paper are pertinent to all sorts of surveillance features in the modern world. This paper should serve as an impetus for enhancing human rights protection through case law and legal framework in this area, with a view to strengthen democratic values without compromising health and safety concerns.

Keywords

surveillance, secret measures, interception, private life, foreseeability, freedom

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation Prudentov, R. V. (2020). Private life and surveillance in a digital era: Human rights in European perspective. *Digital Law Journal, 1*(2), 41–52. https://doi.org/10.38044/2686-9136-2020-1-2-41-52

Submitted: 10 Jun. 2020, accepted: 12 Jul. 2020, published: 20 Jul. 2020

СТАТЬИ

ЧАСТНАЯ ЖИЗНЬ И СЛЕЖКА В ЦИФРОВУЮ ЭПОХУ: ПРАВА ЧЕЛОВЕКА В ЕВРОПЕЙСКОЙ ПЕРСПЕКТИВЕ

Р.В. Прудентов

Фрешфилдс Брукхаус Дерингер ЛЛП
EC4Y 1HS, Великобритания, Лондон, Флит стрит, 65

Аннотация

Данная статья направлена на выявление основных юридических проблем и эволюции вопросов слежки в Европе в контексте прав человека, с акцентом на практику Европейского Суда по правам человека. Целью исследования является совершенствование и синхронизация правовой материи и правоприменительной практики в данной сфере в России и Европе. Автор проанализировал фундаментальные и самые последние решения Суда, которые могут быть применимы к рассматриваемой тематике, в том числе по аналогии, а также недавние исследования в данной сфере. Данная статья рассматривает, помимо прочего, возможность оспаривания *in abstracto* соответствующего законодательства и практики его применения, законные цели, оправдывающие вмешательство, требования к соответствующему законодательству, ограничения усмотрения властей по вопросам слежки, надлежащий характер органов надзора и объем их полномочий, а также некоторые иные гарантии. Данная статья также обсуждает взаимодействие и баланс между свободой и безопасностью, современные подходы и натянутые отношения ЕС и США по распространенным вопросам слежки. Настоящая статья показывает, что в мире COVID-19 вопросы защиты частной жизни, возникающие в связи с "track and trace" и похожими практиками, уже глубоко исследованы судами, и борьба с COVID-19 возможна через методы слежки с минимальным вмешательством в права человека. Основные проблемы, затронутые в данной статье, применимы к любым формам слежки в современном мире. Данная статья должна служить стимулом для усиления защиты прав человека с помощью судебной практики и правового поля в рассмотренной сфере с целью укрепления демократических ценностей без ущерба здоровью и безопасности.

Ключевые слова

слежка, негласные меры, перехват информации, частная жизнь, предсказуемость, свобода

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Прудентов, Р. В. (2020). Частная жизнь и слежка в цифровую эпоху: права человека в европейской перспективе. *Цифровое право, 1*(2), 41–52. https://doi.org/10.38044/2686-9136-2020-1-2-41-52

Поступила: 10.06.2020, принята в печать: 12.07.2020, опубликована: 20.07.2020

Introduction

It has become increasingly common to speak of the emergence of a surveillance society. Dataveillance, CCTV in public areas, and police officers armed with video cameras at public gatherings form an integral part of our living, with governments and various companies gathering large amounts of personal information and, to some extent, knowing us better than our friends and family.

Governments, civil society, tech companies, and cyber-criminals are constantly involved in an ongoing fight for our data, which is approached through powers, civil rights, revenues, and criminal activities, respectively. By way of mere example, in recent years all over the world, use of encryption in various forms of digital communications has exploded, with governments engaging in a public battle over access to encryption codes and contents of communications with smartphone makers and app developers. Most such battles have proven successful for governments, reinforcing serious privacy and political concerns, but also facilitating international efforts in combating terrorism, drugs, weapons, money trafficking, and other crimes.

On account of the European Convention on Human Rights and other similar pieces of law around the world on national and supranational levels, all surveillance activities, regardless of their justification, should be scrutinised in terms of their cost to personal and political freedom, as well as in maintaining democratic values. Notably, the most constant thing in life is change, whereas law (including law-making and law enforcement) is generally conservative, slow, and incremental by its very nature: it takes time to craft, and it quickly becomes outdated in the face of rapid technological and social change (Goold, 2010). These concerns prove topical in the digital area of life in general and surveillance in particular; that fact makes this paper pertinent to several new dimensions of surveillance practices addressed herein.

The European Court of Human Rights (hereinafter the "Court") has contributed greatly to the development of a legal framework for surveillance. The influence and authority of the Court is universally acknowledged, and its case law is prone to adapt (albeit sometimes belatedly) to various social and technological changes. Notwithstanding notorious political pitfalls, the Court's jurisprudence plays a remarkable role in providing the impetus for implementing best practices in a human rights context in Europe, including in the areas of respect for the private life and surveillance.

This paper focuses on identifying key legal considerations and profound human rights law developments in the area of surveillance in Europe (with emphasis on the Court's jurisprudence), with the aim to facilitate the enhancement of this regime in Russia and elsewhere in the world.

Methodology

This paper focuses on the jurisprudence of the Court on several pervasive topics that should be considered by lawmakers and practitioners in the course of applying, enforcing, challenging, or defending various surveillance measures in different circumstances. The choice of case law for analysis was based on author's experience in teaching ECHR law, numerous Court decisions, and commentaries by multiple scholars and practitioners. The format of this paper naturally circumvents detailed analyses and discussions of many topics, each of which may warrant an entire research article. By the same token, selected highlights of international legal considerations and suchlike surrounding modern surveillance human rights issues were chosen based on their timeliness and pivotal nature,

each deserving (and gaining) separate scientific discussions. The above factors contributed to the use of comparative (involving critical analysis of different bodies of law considered by the Court), empirical (involving designing and analysing key legal issues arising in the surveillance context), and doctrinal (involving analysis of the letter of the Court's case law) legal research methodology.

Results

Interference with Private Life

It goes without saying that surveillance can invade a person's private space. Whether or not surveillance interferes with "private life" depends on the circumstances. To set the scene, the Court has consistently emphasised that "private life" is a "broad concept not susceptible to exhaustive definition"[1] and interpreted this notion in various instances. The surveillance issues discussed in this paper concern two primary categories of interest within 'private life' decisions: freedom from interference with physical and psychological integrity, plus the collection and disclosure of information.

The Court acknowledged that the monitoring of an individual's actions in a public place does not, as such, give rise to any interference with that individual's private life, but the recording and subsequent use of the data (and the systematic or permanent nature of the record) may give rise to such considerations[2]. For instance, in 2003, the disclosure of the CCTV footage showing an applicant's attempted suicide to the media constituted a disproportionate and unjustified interference with the applicant's private life[3].

Importantly in the current circumstances, the Court recently recognised that non-covert surveillance in public may also constitute an interference with private life. This was in connection with video surveillance in a university amphitheatre, where professors interact with students and thus develop mutual relations and construct their social identities[4].

The Court accepted that GPS surveillance is less intrusive than other methods of visual or acoustical surveillance, but nevertheless found that GPS surveillance and the processing and use of the data obtained thereby amounts to an interference in private life[5].

Challenge *in Abstracto*

As a matter of fact, it may be difficult for a person to prove that their communications have been intercepted, or that they have been subject to surveillance, given the very secrecy of these activities. Considering this, the Court ruled that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or laws permitting such measures, without having to allege that such measures were in fact applied to them. In other words, in cases concerning secret measures, the Court has allowed individuals the right to challenge a law *in abstracto*[6].

At a later stage, the Court expanded this, claiming it applies only where there are no effective domestic remedies, and thus a widespread suspicion and concern among the general public that

1 *Peck v. the United Kingdom*, ECHR (2003)
2 *Peck*, 2003
3 *Peck*, 2003
4 *Antović and Mirković v. Montenegro*, ECHR (2017)
5 *Uzun v. Germany*, ECHR (2010)
6 *Klass and Others v. Germany*, ECHR (1978)

secret surveillance powers are being abused cannot be said to be justified[7]. In that context, the effectiveness of remedies is genuinely undermined by the absence of a requirement to notify the subject of interception, or an adequate possibility of requesting and obtaining information about secret measures from the authorities[8]. The scope of the legislation permitting secret surveillance measures should also be examined to ascertain whether the applicant could possibly be affected by it.

Otherwise, where effective remedies pertaining to secret measures exist, applicants must meet a fairly low test of demonstrating that they are "potentially at risk of being subjected to such measures"[9].

Legitimate Aims

Surveillance — or other secret measures amounting to interfering with the right to respect for private life, home or correspondence — may be justified by reference to the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others, as per Article 8 (§ 2) of the European Convention on Human Rights. The Court has considered various legitimate aims on many occasions.

One of the illustrative cases herein involved storage of information, for some of the above purposes, on the secret police register, pertaining to the applicants' private lives. It was kept on record as bomb threats made in 1990 by the first applicant and certain other persons were relevant, and proved sufficient reasoning as regards the aim of preventing disorder or crime. By contrast, no legitimate aims described above could be validly asserted in connection with the continued storage of the information concerning (i) the second applicant's participation in a political meeting in Warsaw in 1967, (ii) the third and fourth applicants' membership of the Marxist-Leninist (Revolutionaries) Party, and (iii) an allegation that the fifth applicant had advocated violent resistance to police control during demonstrations in 1969[10].

Necessity

More than 40 years ago, when considering these matters for the first time, the Court already acknowledged that democratic societies found themselves "threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able ... to undertake the secret surveillance of subversive elements operating within its jurisdiction". On this basis, the Court accepted that "the existence of some legislation granting powers of secret surveillance ... is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime"[11].

Therefore, domestic legislature enjoys a certain (but not unlimited) discretion as concerns the fixing of the conditions and procedures under which the system of secret surveillance is to be operated. However, such a law poses a risk of "undermining or even destroying democracy on the ground of defending it", and so states may not adopt whatever measures they deem appropriate. There must be "adequate and effective guarantees against abuse" implemented, depending on the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the

7 *Kennedy v. the United Kingdom*, ECHR (2010)
8 *Roman Zakharov v. Russia*, ECHR (2015)
9 *Roman Zakharov v. Russia*, ECHR (2015)
10 *Segerstedt-Wiberg and others v. Sweden*, ECHR (2006)
11 *Klass*, 1978

authorities competent to permit, carry out, and supervise such measures, and the kind of remedy provided by national law (*Klass and Others v Germany*, 1978).

Notably, with respect to GPS surveillance, the purpose and necessity still need to be considered. Such requirements were deemed satisfied, for example, in a 2010 case, where the investigators had first attempted measures which interfered less with private life, and only then, within three months, then conducted GPS surveillance (and essentially only at weekends, and when the suspect was travelling in his accomplice's car); this was in connection with very serious crimes (attempted murders of politicians and civil servants by bomb attacks)[12].

Legality

Whereas surveillance measures were originally analysed from the perspective of necessity (see above), the issue was subsequently considered in the context of the overlapping notion of legality, i.e. that such measures should be applied "in accordance with the law", meaning, generally, a sufficiently clear and precise legal and procedural framework is in place.

First, the impugned measure should have some basis in domestic law and be compatible with the rule of law, such that the law must thus meet quality requirements: it must be accessible to the person concerned and its effects should be foreseeable[13]. These requirements are not met where, at the very least, surveillance is regulated merely by administrative practice, the details of which are not published, so that the Court is unable to say "with any reasonable certainty" what powers are incorporated in legal rules and what elements remain within the discretion of the executive[14]. It is worth mentioning here a recent (and patently outrageous) Turkish case where the judiciary failed to follow ("flagrantly failed to observe") even the basic requirements of the law when ordering the relevant interception. Such approach is obviously unacceptable[15].

The "foreseeability" element in the context of surveillance measures bears a specific connotation. A person should not be able to foresee when the authorities are likely to intercept their communications. On this basis, there should be no rule providing for advance warning in relation to surveillance, where to do so would threaten the object of such surveillance[16]. It is evident, nevertheless, that the executive's secret exercise of powers may be arbitrary. Therefore, the Court established that the law must be sufficiently clear to adequately indicate the circumstances in which, and the conditions on which, public authorities are empowered to resort to any such measures[17].

Discretion and Supervision

Given that the implementation of secret surveillance measures is not open to scrutiny by the individuals concerned nor the public at large, the competent authorities (i.e., the executive or a judge) should not enjoy unfettered powers, and the law should indicate the scope of their discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference[18]. Those provisions of the law should have a binding force circumscribing discretion in the application of such measures (*Valenzuela Contreras v Spain*, 1998).

---

12 *Uzun*, 2010

13 *Malone v. the United Kingdom*, ECHR (1984); *Rotaru v. Romania*, ECHR (2000); *Kennedy*, 2010

14 *Malone*, 1984

15 *Mustafa Sezgin Tanrikulu v. Turkey*, ECHR (2017)

16 *Mersch and Others v. Luxembourg*, ECHR (1985)

17 *Malone*, 1984; *Leander*, 1987; *Rotaru*, 2000

18 *Malone*, 1984; *Leander*, 1987

The rule of law also implies that any interference by the executive authorities should be subject to effective control by democratic and/or independent institutions, which should normally be assured by the judiciary (at least at the last resort), with judicial control offering the best guarantees of independence, impartiality, and proper procedure. Supervision by non-judicial bodies may be acceptable where such bodies are independent and are vested with sufficient powers and competence[19].

Supervision of the English RIPA regime[20] was considered satisfactory, and it may be treated as an example of acceptable supervision arrangements that are worth highlighting here for reference. First, intercepting agencies were required to keep detailed records of interception warrants that were periodically reviewed by them and, where appropriate, by the Secretary of State. Second, an independent (of the executive and the legislature) office of the Interception of Communications Commissioner was established for overseeing the general functioning of the surveillance regime and the authorization of interception warrants in specific cases. The Commissioner reported annually to the Prime Minister, and his report was laid before Parliament. In addition, any person who suspected interception of their communications could apply to the Investigatory Powers Tribunal (hereinafter "IPT"), with it also being an independent and impartial body that has adopted its own rules of procedure. Both the Commissioner and the IPT had access to all relevant (including closed) documents and material, and each of them comprised of persons who hold or have held high judicial office (or, in the case of the IPT, have been experienced lawyers). The IPT also had powers to quash any interception order, to require the destruction of intercepted material, or to order compensation to be paid. Both the Commissioner's report and the IPT's legal rulings were available to the public, and thus open to public scrutiny[21].

By contrast, the Court found that no meaningful supervision regime existed in Russia. Logging or recording interceptions was prohibited, which made it impossible for any supervising authority to discover unlawful interceptions. At the same time, the law enforcement authorities were technically able to directly intercept all communications. Moreover, judicial supervision was limited to the initial authorization stage, with subsequent supervision being entrusted to the President, Parliament, the Government, the Prosecutor General, and competent lower-level prosecutors. For the first three bodies, there were no regulations or instructions describing the scope, procedures, and conditions for their review, or for remedying the breaches. In theory, there was a legal framework for some supervision by prosecutors of secret surveillance measures; however, prosecutors lacked independence, given that they were appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities, and noting that they also gave approval to requests for interceptions. Moreover, the scope of their supervision was limited; information about the security services' undercover agents, and about the tactics, methods, and means used by them, was outside the scope of prosecutors' supervision. Interceptions performed by the FSB in the sphere of counter-intelligence could be inspected only following an individual complaint that was unlikely to ever be lodged (given that individuals were not notified of interceptions). Supervisory activities were not open to public

[19] *Klass*, 1978

[20] This was the regime established under the Regulation of Investigatory Powers Act 2000. Note that this regime has been substantially modified over time; notably, an office of the Interception of Communications Commissioner was repealed by the Investigatory Powers Act 2016, s 240(1)(a) and (2)(a), with effect from 1 September 2017. The relevant review powers now lie with the Investigatory Powers Commissioner. Investigatory Powers Act, Part 8 (2016).

[21] *Kennedy*, 2010

scrutiny in Russia, as prosecutors' biannual reports were confidential documents that were submitted to the Prosecutor General only and contained statistical information only[22].

On a similar prominent case related to members of a non-governmental 'watchdog' organisation voicing criticism of the Hungarian government, the system of supervision (that was eminently political, and carried out by the Minister of Justice) was found inadequate. Although this Minister was formally independent of both the police force and of the Minister of Home Affairs, he was "inherently incapable of ensuring the requisite assessment of strict necessity"[23].

In short, the level of scrutiny over the surveillance control systems would depend on the scope, manner, and origins of surveillance; furthermore, however, generally speaking, the independence of the oversight body, its jurisdiction, its power to access data, and its power to effective reactions are pivotal in ensuring the rule of law, and hence the compatibility of surveillance with the principles of human rights (Malgieri & De Hert, 2017).

Other Safeguards

More specifically, a few minimum safeguards should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception or another surveillance order; a definition of the categories of people subject to surveillance; a limit on the duration of surveillance; the mandatory procedure for examining, using, sharing, storing, or destroying the data obtained; the precautions to be taken when communicating the data to others; and the circumstances in which recordings may or must be destroyed or otherwise extinguished[24].

In addition to all of the above, appropriate safeguards may also involve "provisions designed to reduce the effects" of any interference "to an unavoidable minimum", and certain limits on the use of information (such as public prosecution and obtaining of citizenship)[25].

The approach taken by Western democracies proves that the publication of information concerning rules and procedures for dealing with intercepted material and other surveillance projects is essential in a democratic society, and should not be viewed as damaging the efficacy of the intelligence-gathering system or otherwise giving rise to a security risk. The German Law of 13 August 1968 on restrictions on the secrecy of mail, post, and telecommunications (hereinafter the "G10 Act") is a widely cited example of democratic enactments in this area. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order, and which search terms had to be listed in the monitoring order. Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail: the authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them, and if that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked, with the destruction having to be recorded in minutes and, in certain cases, having to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention, and use of data obtained through the interception of external communications[26].

---

22 *Roman Zakharov*, 2015

23 *Szabó and Vissy v. Hungary*, ECHR (2016)

24 *Huvig v. France*, ECHR (1990); *Liberty and Others v. United Kingdom*, ECHR (2008); *Roman Zakharov*, 2015

25 *Leander v. Sweden*, ECHR (1987)

26 *Weber and Saravia v. Germany*, ECHR (2006); *Liberty*, 2008

Discussion

Freedom and Security

It is important to recognise the political value of privacy. Reagan argued that privacy is essential to the maintenance of democracy, primarily because it ensures that citizens are able to hold elected governments to account and place limits on the expansion of the state. Unfettered mass surveillance may have a chilling effect on political discourse, creating fears of reprisal. At all times, various forms of surveillance (starting from the census) can be justified on the grounds of safety and security, or as a means to improve public service. These justifications are sometimes treated as mere excuses for an expansion in state power (Goold, 2010).

It is not only governments and secret agencies with the capabilities to possess and produce profoundly pervasive and complicated data mining and information collection, storage, and shaping of surveillance information, but also (and perhaps to a larger extent) the big tech companies, constituting a quarter of the entire US stock market: Amazon, Apple, Google, Facebook, and Microsoft. The desire for security is driving the rampant expansion of government powers of colossal surveillance activity. It is hard to ascertain whether it is possible to say certain things on a cell phone without running afoul of the surveillance systems. The fine balance between freedom and security is uncertain and possibly eventually unsustainable, given rapid changes in the modern world. However, the question is whether this emanates into the concept of a "post democratic" state or not (Barnhizer, 2013).

EU and US: Modern Approaches and Tensions

In the early 21st century, much debate and controversy arose from the terror attacks and the subsequently increased counter-terrorism powers. In Europe, the Data Retention Directive was rapidly adopted; from this, metadata derived from the communications of every individual or legal entity within the EU must be retained and made available for the purpose of "the investigation, detection and prosecution of serious crime", as defined by each Member State (by way of background, "metadata" concerns the context (as opposed to the content) of communication, revealing the 'who', the 'when', the 'what' (type of communication), the 'how' (the device used), and the 'where', combined with results from the aggregation and analysis of this). The revelations made by Edward Snowden in 2013 prompted a global debate concerning the rapid pace of technological developments in the area of communications surveillance and the related privacy implications. Ultimately, in 2014, the Court of Justice of the European Union quashed the aforementioned Data Retention Directive, based on its disproportionate scope (applying to all persons and all means of communication), the length of the retention period, and a lack of provisions ensuring the 'irreversible destruction' of the data or control by an independent authority (Ni Loideain, 2015).

In the US, public privacy discussions in the area of surveillance focus on the need to demonstrate probable cause (or solid grounds and articulable suspicion) before acting, and on whether surveillance constitutes a "search" or "seizure" in the context of the Fourth Amendment (Slobogin, 2002). At the same time, US authorities are notorious for using personal data arbitrarily.

To this end, privacy concerns more and more often are becoming the subject of substantive tensions amongst these countries, and are creating problems for both businesses and government security. For instance, the latest Judgement of the Court of Justice of the European Union quashed the core basis of data transfers from the EU to the US, on the grounds that the limitations on the protection of personal data arising from the US domestic law on the access and use by US public

authorities of such data are not circumscribed by the principle of proportionality, as the surveillance programmes are not limited to what is strictly necessary. In addition, data subjects do not enjoy actionable rights before the courts against the US authorities[27].

Role of Regulators

It has generally been established that private-sector surveillance shapes individuals' reasonable expectations of privacy, and hence regulation of the private sector has effects on the government as a surveillant. On this basis, regulators dealing with private-sector surveillance also affect the stance on civil liberties of the state. Such regulators should make companies more responsible for their surveillance technologies, increase the quality of consent necessary to engage in surveillance, and make companies liable for using certain surveillance techniques and systems (Hoofnagle, 2017).

Lifelogging

Many ideas emerge around the subject of this paper. One worth noting relates to the idea of "lifelogging", referring to a comprehensive archive of an individual's quotidian existence, created with the help of pervasive computing technologies. This is a sort of "time capsule" containing digital archives of a person's lifetime as a means to remember, digest, and possibly use for the best. The emerging interest in this concept obviously stems from the growing capacity to store and retrieve traces of one's own life via digital devices. It is characterized as a combination of personal "sousveillance" (to the extent that it captures data from the perspective of oneself) and surveillance (to the extent it captures data about others that interact with the first person). The resulting memory (in general and in its physical sense) can be a very good thing used for entertainment, sharing, or improving health or personal insight. It may also generate substantive privacy concerns as discussed in this paper (which may be eliminated by ethical limitations and design parameters), not to mention other troubling implications, such as mental and moral health hazards (Allen, 2008).

COVID-19 Considerations

Most recently, digital technologies are being innovatively adopted to combat COVID-19, with various forms of surveillance being exploited (including CCTV, cellular data, and special apps), allegedly for the public good. Any related disclosures of personal information may help to better identify infections and track the spread of the decease.

At the same time, current digital solutions have implications for privacy and data protection. Governments are collaborating with telecom providers to access geolocation data; new mobile applications are also being launched with different degrees of privacy and data protection. Leveraging biometric data has both benefits and challenges. The OECD recommends that governments consider the legal basis of the use of these technologies, which should vary depending on the type of data collected, the requirements of proportionality, transparency, and accountability, and limited time periods for collecting and retaining personal data[28].

The Court's legal positions, outlined above, are vital in considering privacy concerns around anti-COVID-19 digital measures.

---

[27] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, ECLI, CJEU (2020)

[28] Organization for Security and Co-operation in Europe (OECD). (2020, April 23). *Tracking and TRACING COVID: Protecting privacy and data while using apps and biometrics*. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-pro- tecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

Scholars also note that the most privacy-protective app design should be used which meets the public health goal, and the benefits of meeting such a goal outweigh its deleterious effects on privacy. When balancing constitutional values, it is also important to consider the extent by which the app usage reduces the need for restrictions in the form of self-isolation (thus promoting freedom of movement and work) (Austin et al., 2020).

Developed democracies have created solid legal frameworks related to the COVID apps. One example worth noting is Australia, although issues related to the possibility of obtaining this app information by law enforcement agencies and courts remain largely open[29].

Conclusion

Surveys published in several media reveal that many people are concerned about how companies or the government are using their personal data, believing that most of what they do online or while using a cell phone is being tracked by the government, advertisers, and technology firms. Few understand what is being done with their information. When it comes to data collection, people tend to see more risks than benefits.

This paper was meant to outline key human rights considerations arising in the legal area related to surveillance in the modern world. The Court's rulings and international legal framework should hopefully enhance democratic values without compromising health and safety concerns. They should also become the basis for further positive development of laws, case law, and research in this area.

References:

1. Allen, A. L. (2008). Dredging up the past: Lifelogging, memory, and surveillance. *University of Chicago Law Review*, *75*(1), 47–74.
2. Tanguay-Renaud, F., Austin, L. M., Chiao, V., Coleman, B., Lie, D., Shaffer, M., & Slane, A. (2020). Test, trace, and isolate: Covid-19 and the Canadian constitution. *Articles & Book Chapters*, 2797. https://digitalcommons.osgoode.yorku.ca/scholarly_works/2797
3. Barnhizer, D. R. (2013). Through a PRISM darkly: Surveillance and speech suppression in the "post-democracy electronic state" [Unpublished paper]. Cleveland State University. http://works.bepress.com/david_barnhizer/77/
4. Goold, B. J. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In D. W. Schartum (Ed.), *Overvåkning i en Rettsstat – Surveillance in a Constitutional Government* (pp. 38–48). Fagbokforlaget. Allard Research Commons. https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1149&context=fac_pubs
5. Hoofnagle, C. J. (2017). FTC regulation of cybersecurity and surveillance. In D. Gray & S. E. Henderson (Eds.), *The Cambridge handbook of surveillance law*. (pp. 708–726). Cambridge University Press. https://doi.org/10.1017/9781316481127.031
6. Malgieri, G. & De Hert, P. (2017). European human rights, criminal surveillance, and intelligence surveillance: Towards "good enough" oversight, preferably but not necessarily by judges. In D. Gray & S. Henderson

[29] Watts, D. (2020, May 2). *COVIDSafe, Australia's digital contact tracing app: The legal issues*. SSRN Electronic Journal. https://dx.doi.org/10.2139/ssrn.3591622

(Eds.), *The Cambridge Handbook of Surveillance Law* (pp. 509-532). Cambridge University Press. https://doi.org/10.1017/9781316481127.023
7. Moreham, N. A. (2008). The Right to respect for private life in the European Convention on Human Rights: A re-examination. *European Human Rights Law Review*, (1), 44–79.
8. Ni Loideain, N. (2015). EU Law and mass Internet metadata surveillance in the post-Snowden era. *Media and Communication*, *3*(2), 53–62. http://dx.doi.org/10.17645/mac.v3i2.297
9. Slobogin, C. (2002). Public privacy: Camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, *72*, 213-315.

Information about the author:

Roman V. Prudentov — Ph.D. in Law, Solicitor of the Senior Courts of England and Wales, Associate, Freshfields Bruckhaus Deringer LLP, London, UK.
romanprudentov@rambler.ru

Сведения об авторе:

Прудентов Р.В. — кандидат юридических наук, солиситор Высших судов Англии и Уэльса, юрист международной юридической фирмы Freshfields Bruckhaus Deringer LLP, Лондон, Великобритания.
romanprudentov@rambler.ru

https://doi.org/10.38044/2686-9136-2020-1-2-53-66

СТАТЬИ

ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ТЕЛЕМЕДИЦИНЫ

Е.П. Третьякова

Московский офис Юридической компании «Пепеляев Групп»
125047, Россия, Москва, ул. 3-я Тверская-Ямская, 39, стр. 1

Аннотация

Несмотря на то что телемедицина в последние 20 лет активно развивается во всем мире, законодательство зарубежных стран не выработало универсального механизма, позволяющего достичь таких главных целей телемедицины, как удобство, эффективность и доступность.

Вызовы, с которыми столкнулся мир в 2020 году, показали потребность в совершенствовании системы здравоохранения государств, а телемедицинские технологии применялись рядом стран при организации борьбы с новой коронавирусной инфекцией. Такой опыт должен быть воспринят государствами как положительный и использоваться при подготовке законодательных изменений, направленных на совершенствование регулирования телемедицины.

Совместная работа государств в сфере развития телемедицинских технологий позволит сформировать опыт и знания, которые возможно будет использовать при трансформации телемедицинской помощи в трансграничную телемедицину, в том числе посредством принятия актов международного характера.

В процессе исследования автор акцентирует внимание на комплексном регулировании телемедицины. При этом модель телемедицинской помощи, реализованная в Российской Федерации, не является полноценной ввиду отсутствия возможности диагностировать заболевания дистанционно. Такое ограничение влечет возникновение ряда вопросов в других сферах: ответственности доктора, возможности трансграничной медицины, страхового возмещения.

Целью статьи является рассмотрение правового регулирования телемедицинских технологий в Российской Федерации, сравнение отечественного и американского регулирования в соответствующей сфере, а также анализ походов зарубежных исследователей.

Ключевые слова

здравоохранение, телемедицина, персональные данные, цифровое здравоохранение, коронавирус, лицензирование

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Благодарности	Благодарность Руководителю практики здравоохранения юридической фирмы «Пепеляев Групп» Панову А.А. за неоценимую помощь при подготовке исследования.
Для цитирования	Третьякова, Е. П. (2020). Правовые аспекты регулирования телемедицины. *Цифровое право, 1*(2), 53–66. https://doi.org/10.38044/2686-9136-2020-1-2-53-66

Поступила: 27.05.2020, принята в печать: 17.06.2020, опубликована: 20.07.2020

ARTICLES

LEGAL ASPECTS OF TELEMEDICINE

Ekaterina P. Tretyakova

Healthcare Practice at Pepeliaev Group Law Firm, Moscow
Building 1, 39, 3rd Tverskaya-Yamskaya str., Moscow, Russia, 125047

Abstract

Although distance medicine has been actively developing worldwide over the past 20 years, no universal mechanism of legislation has been developed across foreign countries to achieve main goals of tele-health services: convenience, effectiveness, and accessibility.

The need to improve states' healthcare systems has increased after dealing with the challenges that the world faced in 2020. While organizing the fight against the spread of the coronavirus infection, a number of countries invoked telemedicine technologies. The experience of using e-health in difficult epidemiological situations should be perceived by states as positive and thus incorporated when preparing legislative changes aimed at improving the regulation of telemedicine.

States should act jointly in relation to the development of remote medical care technologies. This will help to build up experience and knowledge that can be used in the future when transforming telemedical assistance into cross-border practice, including the adoption of international acts.

Telemedicine should be regulated comprehensively, instigating legal regulations for such issues as medical care provision, digital technologies, medical insurance aspects, licensing, and the protection of personal data. As for the Russian Federation, the remote medicine care model implemented in the country is incomplete due to the inability to diagnose diseases remotely. Such a restriction entails the appearance of a number of questions in other areas: the responsibility of the doctor, the possibilities of cross-border medicine, or insurance compensation issues.

The purpose of the article is to describe the legal regulation of telemedicine technologies in the Russian Federation, comparing Russian regulation with American experiences, and analyzing the main approaches taken by foreign researchers.

Keywords

healthcare, telemedicine, personal data, digital healthcare, coronavirus, licensing

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
Acknowledgments	Thanks to A. Panov the Head of Commercial Practice, Life Sciences of the law firm Pepeliaev Group for invaluable assistance in preparing the study.
For citation	Tretyakova, E. P. (2020). Legal aspects of telemedicine. *Digital Law Journal, 1*(2), 53–66. https://doi.org/10.38044/2686-9136-2020-1-2-53-66

Submitted: 27 May 2020, accepted: 17 Jun. 2020, published: 20 Jul. 2020

Введение

Четвертая промышленная революция дала миру цифровые технологии, возможность осуществления взаимодействия в мировом контексте с использованием разнообразных средств связи. Такие возможности не ограничены местом нахождения и позволяют осуществлять коммуникацию между сторонами, находящимися в разных частях планеты.

Влияние цифровых технологий на медицинскую деятельность нельзя недооценивать. Появляются новые способы сбора и учета информации о пациентах — так называемые информационные системы, появляется программное обеспечение, позволяющее заменить медицинские карты на материальных носителях на электронные медицинские карты, все больше стран внедряют технологии искусственного интеллекта при оказании медицинской помощи.

Отдельным направлением, получившим законодательное закрепление во многих государствах, является телемедицина. В условиях повышения качества жизни у общества повышается спрос на получение квалифицированной медицинской помощи, а также проявляется повышенный интерес к состоянию здоровья. Некоторые ученые называют телемедицину седьмой революцией в сфере здравоохранения (Bauer & Ringel, 1999).

Дать определение телемедицине сложно, в первую очередь это связано с прогрессивным развитием данного направления в последние годы, также разнообразием форм, в которых она проявляется.

В 2010 году Всемирная организация здравоохранения (далее — ВОЗ) насчитала 104 определения телемедицины в государствах-членах и предложила универсальное определение[1], которое на самом деле не изменило существа определений, используемых в нормативных актах государств-членов. Тем не менее специалисты ВОЗ также подчеркнули, что одной из проблем телемедицины представляется недостаточность правового регулирования[2]. Юридические вопросы в сфере телемедицины остаются актуальными и по сей день.

Несовершенство правового регулирования телемедицины в большей степени обусловлено двумя причинами: 1) явление представляется новым для сферы здравоохранения, медицинское сообщество и регуляторы не определились с пределами возможностей телемедицины и рисками, возникающими при ее внедрении; 2) комплексный характер регулирования требует соблюдения не только так называемого «медицинского» законодательства, но и лицензионных требований, требований в сфере защиты персональных данных, обеспечения врачебной тайны.

Рассуждая о телемедицине, необходимо помнить, что ее можно понимать в широком и узком смыслах. Телемедицина в узком смысле с учетом законодательства ряда государств представляет собой взаимодействие 1) «пациент — врач» и 2) «врач — врач».

Телемедицина в широком смысле (telehealth) определяется как отрасль отношений, возникающих в связи с использованием цифровых средств для получения информации о здоровье, состоянии человека, иных данных, источником которых является организм человека. Сюда могут быть отнесены программы, обобщающие информацию о здоровье (например, мобильное приложение), или же программы, которые направлены на расчет необходимой

[1] Всемирная организация здравоохранения. (2012). *Телемедицина. Возможности и развитие в государствах-членах. Доклад о результатах второго глобального обследования в области электронного здравоохранения.* (Серия «Глобальная обсерватория по электронному здравоохранению» (Т. 2)). https://apps.who.int/iris/bitstream/handle/10665/44497/9789244564141_rus.pdf

[2] Там же.

доли принимаемых препаратов, например как это делают помпы, контролирующие уровень сахара в крови и сообщающие через специальное мобильное приложение о необходимой дозировке инсулина.

Распространение в 2020 году новой коронавирусной инфекции столкнуло ряд государств лицом к лицу с проблемами, связанными с организацией здравоохранения. Из-за ограничений, введенных в целях уменьшения случаев распространения коронавирусной инфекции, медицинские учреждения наряду с другими организациями приостановили свою деятельность в части плановых посещений (осмотров). Кроме того, граждане в силу введенных ограничений на свободу перемещения лишились возможности посещения врачей. При этом потребность в получении медицинской консультации не становится меньше, наличие ограничений еще раз подтверждает востребованность телемедицины, преимущества ее дистанционного характера. В соответствии с исследованием консалтинговой компании Frost & Sullivan's в 2020 году прогнозируется рост спроса на телемедицинские услуги в США на 63,4 %[3].

Однако, несмотря на то что направление телемедицины появилось на рубеже XX–XXI веков, по сей день существуют проблемы, связанные с правовым регулированием отрасли.

Законодательство о телемедицине представляет собой совокупность нормативных правовых актов, регулирующих отношения в сфере здравоохранения с использованием информационно-коммуникационных технологий при взаимодействии врача и пациента и (или) взаимодействии врачей между собой. При этом на такие отношения всегда распространяется законодательство, регулирующее оказание медицинской помощи, информационные технологии, защиту информации, а также иные вопросы.

Сами по себе нормы законодательства как отечественного, так и зарубежных стран, посвященные телемедицине, представляют собой массив регулирования, имплементированный в акты по вопросам здравоохранения. В связи с этим возникают проблемы регулирования телемедицинских технологий, к которым относятся: экстерриториальный характер медицинской помощи, оказываемой посредством телемедицинских технологий, особенности лицензирования телемедицинской помощи, защита персональных данных при обработке оператором телемедицинской системы; ответственность врача за действия, связанные с оказанием и (или) консультированием с использованием телемедицинских технологий.

Возникающие в результате внешних факторов ограничения и объективная отдаленность пациента от необходимого ему специалиста и возможность использования телемедицины не должны создавать рисков для здоровья граждан, по этой причине требуется специальное нормативное регулирование, учитывающее соблюдение и гарантии основных прав граждан.

К примеру, должна быть обеспечена защита персональных данных пациента, а также соблюдение врачебной тайны. Таким образом, возникает необходимость в законодательном закреплении норм, предъявляющих требования к разработчикам телемедицинских систем, их операторам, компаниям, осуществляющим сервисное обслуживание. При этом нормы должны быть подкреплены мерами государственного принуждения, и за их нарушение должны быть предусмотрены санкции. Таким образом, будет усиливаться конкуренция на рынке телемедицинских технологий и сопутствующих ему рынках.

При использовании телемедицинских технологий может возникнуть ряд технических сложностей, которые не могли предвидеть врач или пациент.

---

[3] Frost and Sullivan. (2020). *Telehealth—a technology-based weapon in the war against the coronavirus* [Телемедицина — технологичное оружие в борьбе с коронавирусом]. https://go.frost.com/NA_PR_TH_MFernandez_K488_Telehealth_May20

Если смотреть в перспективу развития телемедицины, то медицинский работник, осуществляющий консультирование в рамках оказания телемедицинской помощи, должен иметь гарантии и нести ответственность за свои действия, как и медицинские работники, оказывающие помощь очно. В настоящее время следует учитывать, что в реалиях отечественного регулирования телемедицина не является самостоятельным видом медицинской помощи, а представляет собой лишь информационно-коммуникативное взаимодействие между пациентом и врачом либо до первого очного приема, либо после такого приема.

Описанные выше проблемы и текущая мировая ситуация требуют рассмотрения вопросов правового регулирования телемедицинских технологий, анализа отечественного и зарубежного опыта, а также формирования предложений по совершенствованию правовых норм, регулирующих телемедицину.

Методология исследования

В рамках настоящего исследования основным методом при изучении актов, направленных на регулирование телемедицины, был аналитический метод.

Выбор аналитического метода обусловлен тем, что телемедицина представляет собой комплексный институт, который необходимо рассматривать через призму законодательства и базовых учений о правовом регулировании здравоохранения, персональных данных, иных аспектов, которые применимы как в телемедицине, так и при очном взаимодействии врача и пациента.

При рассмотрении практики внедрения телемедицинских технологий в зарубежных странах использовались аналитический и сравнительный методы.

Выбор сравнительно-правового метода обусловлен изучением нормативных правовых актов, регулирующих телемедицинские технологии в зарубежных странах и в Российской Федерации, с целью формирования общих тенденций регулирования телемедицины, выделения различий в сфере телемедицинских технологий, а также формирования положений о текущей ситуации в сфере мировой телемедицины.

Результаты исследования

По результатам проведенного исследования автор приходит к выводу, что современный этап регулирования телемедицинских консультаций находится на стадии развития.

Правовые акты, направленные на регулирование смежных вопросов, требуют совершенствования, а модель телемедицины, закрепленная в Российской Федерации, должна развиваться в сторону легального разрешения дистанционной диагностики.

Пандемия, на наш взгляд, показала востребованность медицины и еще раз подчеркнула ограничения и проблемы, которые есть в текущем регулировании. Мы полагаем, что борьба с коронавирусной инфекцией станет катализатором для ускоренного развития телемедицины и соответствующих изменений законодательства.

Дискуссия

Телемедицина как элемент цифрового здравоохранения: статус телемедицинских консультаций в Российской Федерации

В Российской Федерации о развитии телемедицины речь шла с начала 2000-х годов. В 2001 году Министерство здравоохранения Российской Федерации совместно с Российской академией медицинских наук утвердило Концепцию развития телемедицинских технологий в Российской Федерации[4]. Указанный документ рассматривал телемедицину как «медицину на расстоянии» и ставил целью не только развитие взаимодействия «врач — пациент» и «врач — врач», но и усовершенствование образовательных технологий, возможностей проведения экзаменов и тестирования, перспектив взаимодействия врачей со спасателями и др. Среди первоначальных задач телемедицины в рамках концепции стояли следующие направления:

- консультации сложных больных на различных этапах оказания помощи;
- экстренные консультации больных, находящихся в критическом состоянии;
- консультации в процессе оказания помощи пострадавшим в чрезвычайных ситуациях;
- догоспитальное консультирование больных для уточнения предварительного диагноза / метода лечения и решения вопроса о месте и сроках предстоящего лечения.

В течение последующих десяти лет нормативных правовых актов, направленных на развитие телемедицины, не принималось. И только 29 июля 2017 года был принят Федеральный закон № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»[5], легально закрепивший телемедицину в Российской Федерации. Указанными изменениями была введена в Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[6] (далее — 323-ФЗ) статья 36.2, в которой описываются особенности медицинской помощи, оказываемой с применением телемедицинских технологий. Во исполнение данной нормы Министерством здравоохранения был утвержден Порядок организации и оказания медицинской помощи с применением телемедицинских технологий[7].

Следует отметить, что введение телемедицины было не единственным шагом к цифровизации здравоохранения, одновременно с этим было утверждено регулирование, положившее основу для Единой государственной системы в сфере здравоохранения, а также для электронных рецептов на лекарственные препараты.

Определение телемедицины как таковое в 323-ФЗ отсутствует. Близким представляется подход ВОЗ, который определяет электронное здравоохранение как «использование информационных и коммуникационных технологий (ИКТ) для здравоохранения»[8].

Отечественный законодатель также отталкивался от ключевого значения применяемых технологий. Действующая редакция 323-ФЗ дает следующую дефиницию телемедицинским техно-

[4] Приказ Минздрава РФ № 344, РАМН № 76 от 27.08.2001 «Об утверждении Концепции развития телемедицинских технологий в Российской Федерации и плана ее реализации». Документ опубликован не был.

[5] СЗ РФ, 31.07.2017, № 31 (Часть I), ст. 4791.

[6] СЗ РФ, 2011, № 48, ст. 6724.

[7] *Приказ* Минздрава России № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий» (2017).

[8] World Health Organization [Всемирная организация здравоохранения]. (n.d.). eHealth [Электронное здравоохранение]. https://www.who.int/ehealth/en/

логиям: «*информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента*».

Исходя из представленного легального определения, мы можем выделить два уровня взаимодействия с использованием телемедицинских технологий: вертикальный и горизонтальный. Вертикальный уровень представляет собой взаимодействие «врач — пациент» и рассматривается как ключевой в рамках настоящего исследования. Горизонтальный уровень представляет собой взаимодействие между врачами, проведение консилиумов, консультаций и иного взаимодействия.

Важно обратить внимание на то, что современное регулирование в Российской Федерации не относит телемедицину к условиям, в которых может быть оказана медицинская помощь (вне медицинской организации, амбулаторно, в дневном стационаре, стационарно). Статья 36.2 323-ФЗ устанавливает закрытый перечень случаев, когда возможна консультация пациента:

1) случаи профилактики, сбора, анализа жалоб пациента и данных анамнеза, оценки эффективности лечебно-диагностических мероприятий, медицинского наблюдения за состоянием здоровья пациента;

2) случаи принятия решения о необходимости проведения очного приема (осмотра, консультации).

Таким образом, текущий подход 323-ФЗ предусматривает использование телемедицины исключительно в информационных целях, то есть в рамках телемедицинской консультации врач не может осуществлять коррекцию раннее назначенного лечения или диагноза без очного осмотра. Наблюдение за состоянием здоровья пациента также возможно только после очного приема. Исходя из описанного выше механизма, отечественная телемедицина не позволяет без очного посещения врача определить заболевание и получить назначенное лечение. Очевидно, что такая форма должна перерасти в самостоятельную форму оказания медицинской помощи на основании практики, достижений технологий и учета профессионального мнения медицинского сообщества. В свою очередь, не для всех направлений медицины возможна постановка диагноза дистанционно, тем не менее в некоторых зарубежных государствах допускается при постановке диагноза использовать телемедицину. Это касается гриппа, ангины, различных инфекций, в том числе респираторных, синусовых и других заболеваний (Halpren-Ruder et al., 2019).

Поскольку целью телемедицины является не только облегчение работы врачей, но и обеспечение доступности медицины в труднодоступной местности, то потребность в дистанционной диагностике необходима.

Если обратиться к статистике, можно увидеть, что не все пациенты, получившие первичную консультацию с использованием телемедицинских технологий, обращаются к доктору повторно. Только 20 % пациентов после личного приема используют телемедицинские технологии для продолжения взаимодействия с врачом. Если первичным был онлайн-прием, то количество последующих обращений варьируется в пределах 6 % (Vladzimirsky, 2018). Такие показатели можно объяснить тем, что установить диагноз и получить соответствующее назначенное лечение от врача можно *только при очном приеме*, а если диагноз не поставлен в рамках телемедицинской консультации, то пациент воспользуется традиционным способом получения

консультации и необходимость в последующем обращении с использованием телемедицины отпадает. Последующее обращение с помощью телемедицинских технологий несет цель поддержания коммуникации с врачом и сопровождение процесса лечения. После очного посещения врача лицо, которое ранее не обращалось за телемедицинской консультацией, с наибольшей вероятностью обратится за ней для поддержания процесса лечения, а не с целью получения такого лечения.

В период пандемии депутатами поднимался вопрос о внесении изменений в 323-ФЗ, направленных на возможность установления предварительного диагноза в рамках телемедицинской консультации[9]. Однако инициатива не была реализована.

В условиях распространения коронавирусной инфекции развития законодательства в сфере телемедицины на федеральном уровне не произошло. Тем не менее на региональном уровне использовался механизм телемедицины для оперативного получения информации и дачи консультаций лицам с подтвержденной коронавирусной инфекцией. Ярким примером использования телемедицинских возможностей является Приказ департамента здравоохранения города Москвы от 6 апреля 2020 г. № 356 «О применении телемедицинских технологий при организации оказания консультаций по вопросам коронавирусной инфекции COVID-19 и подборе персонала в медицинские организации города Москвы» (далее — Приказ)[10]. В соответствии с Приказом на территории г. Москвы был создан Телемедицинский центр для предоставления дистанционной консультативной медицинской помощи пациентам с подтвержденной коронавирусной инфекцией. Среди основных задач телемедицинского центра выделено:

- оценка состояния здоровья пациента на основании анализа жалоб и данных анамнеза;
- мониторинг состояния пациентов, в отношении которых проводились консультации с применением телемедицинских технологий;
- оценка эффективности лечебно-диагностических мероприятий;
- динамическое медицинское наблюдение за состоянием здоровья пациента;
- принятие решения о необходимости проведения очного осмотра врачом поликлиники или врачом бригады скорой медицинской помощи для госпитализации в стационар круглосуточного наблюдения;
- принятие решения о необходимости коррекции ранее назначенного лечения врачом при очном осмотре;
- сбор, обработка и анализ полученных статистических данных об оказании консультативной медицинской помощи пациентам с подтвержденной коронавирусной инфекцией COVID-19, состояние которых позволяет наблюдаться на дому.

Приказ не должен противоречить положениям 323-ФЗ и не дает возможности устанавливать диагноз, однако позволяет централизованно (на уровне региона) оказывать консультативное содействие одной группе пациентов. Такие меры позволили решить проблему переполненных больниц, а также предоставить возможность большому количеству граждан оценить плюсы

[9] Znak. (2020, Март 24). *В Госдуме вспомнили о телемедицине: очень нужна в период эпидемий*. https://www.znak.com/2020-03-24/v_gosdume_vspomnili_o_telemedicine_ochen_nuzhna_v_period_epidemiy

[10] Приказ Департамента здравоохранения г. Москвы от 06.04.2020 № 356 «О применении телемедицинских технологий при организации оказания консультаций по вопросам коронавирусной инфекции COVID-19 и подборе персонала в медицинские организации города Москвы» (вместе с «Положением о Телемедицинском центре», «Временным регламентом организации оказания консультативной медицинской помощи гражданам города Москвы с подтвержденной новой коронавирусной инфекцией COVID-19, состояние которых позволяет наблюдаться на дому»). Документ опубликован не был.

и минусы телемедицины. Структуры, аналогичные Телемедицинскому центру, могут быть созданы на уровне регионов не только в целях борьбы с коронавирусной инфекцией, но и для оказания консультаций для групп пациентов с наиболее распространенными заболеваниями.

Отсутствие возможности осуществлять диагностику заболевания тормозит развитие телемедицины в РФ. В рамках обозначенного вопроса интересно рассмотреть регулирование телемедицины в США[11]. Так, например, законодательство ряда штатов допускает возможность установления диагноза дистанционно (штаты Аляска, Аризона, Колумбия и др.). В то же время законодательство штата Алабама в части установления диагноза имеет некоторые аналогии с российским подходом: диагноз можно устанавливать только после осмотра face-to-face или когда пациент лично посещал другого доктора ранее[12].

Лицензирование и кросс-лицензирование как обеспечение доступности медицинской помощи

Как было указано раннее, телемедицина с точки зрения правового регулирования представляет собой комплексный институт, включающий в себя оказание медицинской помощи, некоторые положения об информации, а также телекоммуникационных технологиях. Все эти аспекты требуют особого внимания, поскольку ключевой целью внедрения телемедицины является обеспечение права граждан на получение медицинской помощи.

Российский законодатель наряду с рядом других требований установил, что телемедицинские услуги может оказывать исключительно организация, обладающая медицинской лицензией. В отечественном законодательстве наличие лицензии позволяет осуществлять деятельность на территории всей страны, например пациент из Москвы может обратиться за телемедицинской консультацией к специалисту, находящемуся и практикующему во Владивостоке. Однако американское законодательство предусматривает иное регулирование.

До недавнего времени практически во всех штатах США наличествовало законодательное положение, позволяющее легально использовать телемедицинские технологии только в случае, если местом нахождения пациента и местом осуществления деятельности врача (место получения лицензии) является один и тот же штат. Специалисты отмечают, что профессиональное лицензирование в таком случае является препятствием для развития телемедицинских технологий и их широкого использования (Becker et al., 2019). Верховным судом Калифорнии оставлено в силе решение нижестоящего суда о привлечении доктора Хегесета к уголовной ответственности за осуществление медицинской деятельности в Калифорнии по лицензии, выданной в штате Колорадо (Hageseth v. Superior Court of San Mateo County). Этот случай подчеркнул необходимость расширения границ при оказании телемедицинских консультаций в США. Указанный процесс состоялся в 2007 году, и по истечении более чем 10 лет законодательство многих штатов было изменено. Однако говорить о единообразии преждевременно. Только 23 государственных медицинских совета штатов выдают лицензии (сертификаты), которые дают возможность практикующим врачам оказывать услуги с помощью телемедицины за пределами штата. Такие лицензии называются cross-state license. На сайте Center for Connected Health Policy (www.

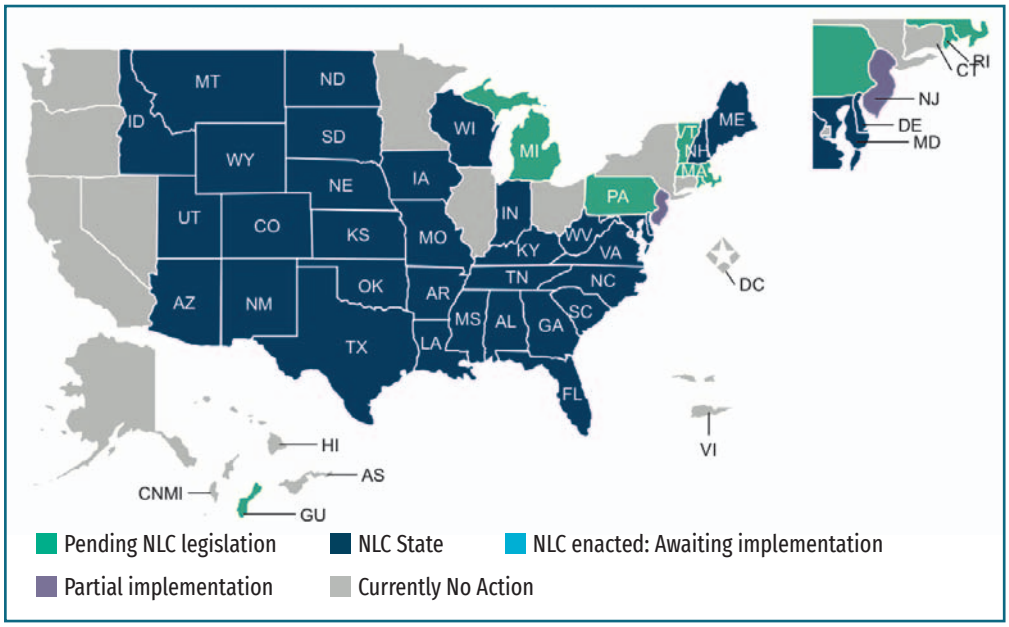
---

[11] В силу федеративного устройства регулирование телемедицинской помощи находится в ведении штатов. Здесь и далее в рамках настоящей статьи необходимо учитывать эту особенность.

[12] Center for Connected Health Policy. (2020). State telehealth laws and reimbursement policies report [Отчет о законодательстве и обеспечении в области телемедицины]. https://www.cchpca.org/telehealth-policy/state-telehealth-laws-and-reimbursement-policies-report

Рисунок 1 / Figure 1

Текущая ситуация Соглашения о лицензировании медсестер в штатах / Current NLC States and Status



Note. Adapted from National Council of State Boards of Nursing. *https://www.ncsbn.org/nurse-licensure-compact.htm*

cchpca.org) представлена актуальная информация о текущем состоянии телемедицины в каждом из штатов, при этом вопрос лицензирования обозначен как один из ключевых пунктов.

По результатам совместной работы штатов было утверждено Соглашение о лицензировании медсестер (Nursing Licensure Compact — NLC), которое позволяет иметь одну лицензию в одном из штатов и практиковать в штатах, которые подписали такое соглашение. Федерация медицинских коллегий (Federal State Medical Boards) разработала текст типового договора о медицинском лицензировании (IMLC), который был принят почти в половине штатов (Chuchvara et al., 2020).

Выше на рисунке 1 представлена текущая ситуация, связанная с имплементацией NLC.

По своей сути, такой подход тормозит развитие телемедицины на глобальном уровне, а также не позволяет достичь целей, поставленных при введении института телемедицины: доступность медицинской помощи сельским жителям, развитие инфраструктуры (Marcoux, & Vogenberg, 2016).

Толчок для развития кросс-лицензирования в 2020 году дала пандемия. На период распространения коронавирусной инфекции 49 штатов отказались от требований о наличии обязательной лицензии в штате, где находится пациент[13]. Мы полагаем, что в регулировании телемедици-

[13] U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19 [Изменение законодательства штатов и требований к телемедицине в ответ на вызовы COVID-19]. (2020). *Federation of State Medical Boards*. https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf

ны во многих штатах наметилась либеральная тенденция. Такие действия можно рассматривать как шаг на пути к трансграничному формату телемедицины и путь к мировому сотрудничеству государств в этой сфере.

Сопутствующее регулирование телемедицинских технологий

Статья 36.2 323-ФЗ обязывает участников дистанционного воздействия в рамках телемедицины осуществлять идентификацию и аутентификацию через Единую систему идентификации и аутентификации (Госуслуги), а также требует наличия у медицинского работника квалифицированной электронной подписи. Такие требования обусловлены цифровым характером рассматриваемого вопроса и позволяют применять уже действующие формы подтверждения и удостоверения личности. Трудности вызывает положение о наличии квалифицированной электронной подписи, поскольку ее получение требуется для внесения информации в медицинскую документацию, а также документирования информации об оказании медицинской помощи пациенту с применением телемедицинских технологий. Процедура получения электронной подписи регулируется Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ[14]. Для получения квалифицированной электронной подписи требуется предоставить необходимые документы в специальный сертифицированный центр, оплатить соответствующую услугу. При этом период действия такой подписи ограничен, как правило, 1 годом. Для полной имплементации телемедицины в систему здравоохранения требуется, чтобы медицинская организация принимала на себя обязанности по получению сотрудниками, работающими с использованием телемедицинских технологий, квалифицированных электронных подписей, а оплата стоимости их получения производилась за счет средств соответствующих учреждений. Затруднений не возникает, когда речь идет о частных медицинских клиниках, чего нельзя сказать о бюджетных медицинских учреждениях (государственных больницах).

Поднимая вопрос финансирования, следует обратить внимание на программы обязательного медицинского страхования. В Российской Федерации система обязательного медицинского страхования имеет два уровня: базовая программа[15], которая имеет федеральное значение, и территориальная программа обязательного медицинского страхования, которая должна предоставлять все объемы медицинской помощи, предусмотренные базовой, а также может быть расширена по усмотрению территориального фонда обязательного медицинского страхования соответствующего региона. На текущий момент базовая программа не включает телемедицину. Регионы на свое усмотрение принимают территориальные программы, покрывающие расходы на телемедицину. Стоимость телемедицинских консультаций варьируется в зависимости от специалиста, к которому обратился пациент. Например, от 959 руб. (офтальмология) до 2772 руб. (эндокринология)[16]. Указанные суммы, как правило, меньше, чем суммы за аналогичный очный прием.

---

[14] «Парламентская газета», № 17, 08–14.04.2011.

[15] Постановление Правительства РФ от 07.12.2019 № 1610 «О Программе государственных гарантий бесплатного оказания гражданам медицинской помощи на 2020 год и на плановый период 2021 и 2022 годов». СЗ РФ, 23.12.2019, № 51 (часть I), ст. 7606.

[16] Коберник, О. (2019, Ноябрь 01). *Телемедицина получила тариф ОМС*. МедВестник. Портал российского врача. https://medvestnik.ru/content/articles/Telemedicina-poluchila-tarif-OMS.html

Отсутствие в базовой программе обязательного медицинского страхования телемедицины позволяет не всем регионам использовать такой инструмент, соответственно это тормозит развитие медицинской инфраструктуры, а также не обеспечивает должным образом доступность медицинской помощи для удаленных регионов и сельской местности.

В отличие от отечественного подхода к возмещению стоимости затрат на телемедицину, некоторые штаты США используют паритет услуг ("service parity")[17], смысл которого заключается в возмещении затрат в том же объеме, как если бы услуга была оказана лично. Настоящий подход является важным в части формирования системы оплаты труда медицинских работников, а также создания системы стимулов для использования телемедицинских технологий.

При удаленном наблюдении за здоровьем пациента врач отвечает за качество оказываемой медицинской помощи. При этом в отечественном законодательстве могут возникнуть сложности по вопросам ответственности за результат консультации с использованием телемедицинских технологий.

В российской литературе есть позиция, согласно которой невозможно привлечь к ответственности за некачественное оказание медицинской помощи врача в связи с тем, что в процессе взаимодействия «врач — пациент» с использованием телемедицинских технологий оказывается информационная услуга, а не медицинская (Bazina, & Simenyura, 2020). На наш взгляд, такая позиция является дискуссионной, поскольку ответственность возникает, когда причинен вред здоровью пациента неправильным диагнозом или назначенным лечением. В соответствии с проведенными исследованиями более чем в 65 % случаев врачи пренебрегли правилами консультирования с использованием телемедицинских технологий и назначили медикаментозное лечение (Morozov et al., 2020). Полагаем, что существующее регулирование, не дающее возможности назначать лечение дистанционно, должно восприниматься специалистами здравоохранения императивно.

Последняя проблема телемедицинских технологий, рассматриваемая в рамках настоящей статьи, — это сохранение врачебной тайны и обеспечение информационной безопасности в целях защиты персональных данных. В связи с тем что между пациентом и врачом при оказании медицинских услуг с использованием телемедицинских технологий возникает третья сторона — оператор, то юрисдикции, допустившие использование телемедицины, должны предусмотреть нормы, направленные на недопущение нарушений со стороны операторов в сфере защиты информации. В противном случае будут нарушены базовые требования к организации здравоохранения.

Проблема защиты персональных данных требует оценки не только со стороны государства, но и со стороны общества. Любопытным представляется исследование, проведенное в 2007 году, которое показало, что здоровые участники были более обеспокоены безопасностью и защищенностью своих данных, чем участники с хроническими заболеваниями (Walker et al., 2009). Такие выводы интересны с точки зрения мотивации пациента и его ценностей, но не должны быть ориентиром для законодателя. Данные о пациентах независимо от состояния их здоровья, наличия сложных заболеваний должны быть защищены в полной мере.

Регулирование деятельности по обработке и использованию персональных данных в России определяется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»[18]. За безопасность персональных данных отвечает оператор системы: организации,

[17] К таким штатам относится Калифорния, Делавэр, Джорджия, Гавайи, Миннесота, Нью-Мексико.

[18] «Парламентская газета», № 126 –127, 03.08.2006.

которые хранят, собирают, передают или обрабатывают персональные данные, должны выполнить ряд технических и организационных требований по защите этой информации. Каждая организация обязана иметь пакет документов, подтверждающих защищенность персональных данных. Однако стандартных мер защиты персональных данных для телемедицины недостаточно.

Оператор в рамках телемедицины может встретить ряд проблем, которые не имеют места в других информационных системах. Это связано с тем, что телемедицинские программы обрабатывают данные о состоянии здоровья, которые являются специальной категорией персональных данных. В силу того что данные о здоровье являются специальными в контексте правового регулирования, имеет место особая форма согласия пациента, в частности, оно должно быть письменным. Очевидно, что такой подход не вписывается в рамки телемедицины и должен быть пересмотрен с учетом цифровизации здравоохранения. Так, например, европейское регулирование допускает получение не только письменного, но и точно выраженного устного согласия[19].

Заключение

Телемедицина является сложным явлением для современного правового регулирования, поскольку необходимо соблюдать баланс между, с одной стороны, внедрением цифровых технологий и, с другой, защитой здоровья граждан, а также обеспечением их информационной безопасности. Данные обстоятельства создают для современного регулятора ряд проблем.

Ключевым недостатком отечественной системы здравоохранения является отсутствие возможности проводить дистанционную диагностику заболеваний. Либерализация законодательства в этой сфере повлекла бы изменения в области защиты персональных данных, а также обязательного медицинского страхования.

Полагаем, что опыт телемедицины, применяемый в условиях распространения коронавирусной инфекции как в Российской Федерации, так и в других странах, откроет новые возможности для технологий и совершенствования правового регулирования.

Список литературы / References:

1. Bauer, J., & Ringel, M. (1999). *Telemedicine and the reinvention of healthcare: The seventh revolution in medicine (healthcare informatics executive management)*. McGraw-Hill.
2. Halpren-Ruder, D., Chang, A., Hollander, J., & Shah, A. (2019). Quality assurance in telehealth: Adherence to evidence-based indicators. *Telemedicine and e-Health, 25*(7), 599–603. https://dx.doi.org/10.1089%2Ftmj.2018.0149
3. Vladzimirsky, A. V. (2018). Effektivnost' telemedicinskih konsul'tacij "pacient–vrach": status praesens [The effectiveness of telemedicine consultations "patient-doctor": Status praesens]. *Journal of Telemedicine and E-Health, 8*(3), 64–70. https://doi.org/10.29188/2542-2413-2019-5-1-31-37
4. Becker, C., Dandy, K., Gaujean, M., Fusaro, M., & Scurlock, C. (2019). Legal perspectives on telemedicine part 1: Legal and regulatory issues. *The Permanente Journal, 23*, 18-293. https://doi.org/10.7812/TPP/18-293

[19] Разъяснения Рабочей группы ЕС по персональным данным. (2019). *Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.* https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/files/2011/wp187_en.pdf

5. Chuchvara, N., Patel, R., Srivastava, R., Reilly, C., & Rao, B. (2020). The growth of teledermatology: Expanding to reach the underserved. *Health Policy and Practice, 82*(4), 1025–1033. https://doi.org/10.1016/j.jaad.2019.11.055
6. Marcoux, R., & Vogenberg, F. (2016). Telehealth: Applications from a legal and regulatory perspective. *Pharmacy and Therapeutics, 41*(9), 567–570.
7. Bazina, O. O., & Simenyura, S. S. (2020). Telemedicina: dostoinstva, nedostatki, realii (pravovoj analiz i prakticheskoe primenenie) [Telemedicine: advantages, disadvantages, realities (legal analysis and practical application)]. *Medical Law, 3,* 32–38.
8. Morozov, S. P., Vladzimirsky, A. V., & Simenyura, S. S. (2020). Kachestvo pervichnyh telemedicinskih konsul'tacij "pacient-vrach" (po rezul'tatam testirovaniya telemedicinskih servisov) [Quality of primary telemedicine consultations "patient-doctor" (based on the results of testing telemedicine services)]. *Physician and Information Technology, 1,* 52–61.
9. Walker, J., Ahern, D., Le, L., & Delbanco, T. (2009). Insights for internists: "I want the computer to know who I am". *Journal of General Internal Medicine, 24*(6), 727–732. https://doi.org/10.1007/s11606-009-0973-1
10. Buyanova, A. V. (2018). Telemedicina problemy regulirovaniya i pravoprimeneniya [Telemedicine regulation and enforcement issues]. *Socio-political sciences, 2,* 235–238.
11. Becker, Chr., Dandy, K., Gaujean, M., Fusaro, M., & Scurlock, C. (2019). Legal perspectives on telemedicine part 2: Telemedicine in the intensive care unit and medicolegal risk. *The Permanente Journal, 23.* https://doi.org/10.7812/tpp/18.294
12. Blue, R., Yang, A., Zhou, C., de Ravin, E., Teng, C. W., Arguelles, G. R., Huang, V., Walthen, C., Miranda, S. P., Marcotte, P., Malhotra, N. R., Welch, W. C., & Lee, J. Y. K. (2020). Telemedicine in the era of coronavirus disease 2019 (COVID-19): A neurosurgical perspective. *World Neurosurgery, 139,* 549–557. https://dx.doi.org/10.1016%2Fj.wneu.2020.05.066

Сведения об авторе:

Третьякова Е.П. — магистр права, юрист практики здравоохранения юридической фирмы «Пепеляев Групп», Москва, Россия.
ek.tretiakova@gmail.com

Information about the author:

Ekaterina P. Tretyakova — Master of Law, Associate of Healthcare Practice at Pepeliaev Group Law Firm, Moscow, Russia.
ek.tretiakova@gmail.com