ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 2, No. 1, 2021

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 2, No. 1, 2021

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 2, № 1, 2021

Contents

Содержание

От редакции

Статьи

Рецензия на книгу

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:	31 Mar. 2021
Copyright:	© Digital Law Journal, 2021
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:	31.03.2021
Копирайт:	© Цифровое право, 2021
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2021-2-1-8-28

EDITORIAL

DIGITAL LAW: THE PURSUIT OF CERTAINTY

Maxim I. Inozemtsev

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

Abstract

The article deals with the development of digital law as an instrument for regulating the digital economy. It is proved that, within the academic environment, the concept of "Internet law" is still more well-established than the concept of "digital law". It is in this manner that the legal sphere responds to the challenges of the digital revolution and reflects the digital economy. The debate as to whether "Internet law" can be considered either as a separate branch of law or as a branch of legislation has not yet subsided. Nevertheless, "Internet law" is undoubtedly an independent academic discipline, textbooks on which are published in Russia. However, Russia needs to develop a digital economy; this is why the national project "Digital Economy of the Russian Federation" was adopted in 2018, regulatory support for which forms the basis of digital law in Russia. At the same time, the extensive experience of digital economy regulation in both its neighbouring countries and beyond is taken into account. Especially attractive is the national strategic model, which assumes the most rapid procedure for adopting changes and consequently adapting digital legislation, is aimed at the long-term perspective, and lets popular opinion — as well as the opinions of public organizations, the business community, and government representatives — be taken into account. In addition to foreign experience in regulating the digital economy, we should also use the best practices of domestic and foreign legal science.

Keywords

digital law, Internet law, digital economy, industrial revolution, national program

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Inozemtsev, M. I. (2021). Digital law: The pursuit of certainty. *Digital Law Journal*, *2*(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Submitted: 21 Jan. 2021, accepted: 15 Feb. 2021, published: 31 Mar. 2021

ОТ РЕДАКЦИИ

ЦИФРОВОЕ ПРАВО: В ПОИСКАХ ОПРЕДЕЛЕННОСТИ

М.И. Иноземцев

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

Аннотация

В статье рассматривается вопрос развития цифрового права как инструмента нормативного регулирования цифровой экономики. Доказывается, что пока более устоявшимся, нежели понятие «цифровое право», в академической среде является понятие «интернет-право». Именно в такой форме правовая сфера отвечает на вызовы цифровой революции и является отражением цифровой экономики. До сих пор не утихли споры, можно ли рассматривать «интернет-право» в качестве отдельной отрасли права или отрасли законодательства. Тем не менее это несомненно самостоятельная академическая дисциплина, учебники по которой издаются уже и в России. Необходимость развития цифровой экономики остро стоит и перед Россией, в этих целях в 2018 г. был принят национальный проект «Цифровая экономика РФ». Нормативное обеспечение реализации данного проекта формирует основу цифрового права в России. При этом учитывается обширный опыт нормативного регулирования цифровой экономики в странах ближнего и дальнего зарубежья. Особенно привлекательной выглядит общенациональная стратегическая модель, которая предполагает наиболее оперативный порядок принятия изменений, следовательно, и адаптации цифрового законодательства, нацелена на долгосрочную перспективу, позволяет учитывать мнение населения, общественных организаций, бизнес-сообщества, представителей власти. Помимо зарубежного опыта нормативного регулирования цифровой экономики необходимо также использовать наработки отечественной и зарубежной правовой науки.

Ключевые слова

цифровое право, интернет-право, цифровая экономика, промышленная революция, национальная программа

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Иноземцев, М. И. (2021). Цифровое право: в поисках определенности. *Цифровое право, 2*(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Поступила: 21.01.2021; принята в печать: 15.02.2021; опубликована 31.03.2021

Object of Investigation

The digital economy and information society inevitably require “digital law” as a tool for regulating public relations online, as well as public relations concerning digital objects in the form of data and knowledge. The specific character of the digital sphere makes it impossible to automatically

apply the existing norms and legal institutions to it. At the same time, the answer to the question of how to adapt the existing legal norms to the digital environment is not obvious and requires scientific reflection by the international legal community.

This task is also complicated by the fact that modern social relations are often hybrid in nature and can be observed simultaneously in two areas: physical and digital. These spheres are deeply embedded within each other, but they are not interchangeable. Digital space rather complements physical space, forming an "augmented reality". However, when describing this interaction, researchers are often tempted to see a zero-sum game: they either declare that the "figure" has completely changed social relations, or that the influence is primarily quantitative, not qualitative, even though the digital sphere itself is formatted by social relations that had developed before it appeared. Attempts to neutralize the relationship between these two spheres and the influence that this interaction has on various aspects of social relations are performed extremely rarely.

The law should take this hybrid into account, considering it not as two separate spheres each with its own logic but as systemic integrity formed by social relations. Khabrieva notes that "it is clearly not enough to state the emergence of a kind of "cross-industry" legal norms that ensure "reinstalling the legal software" to meet the goals and objectives of the digital economy. It is important to understand not only how they will affect public relations, people's will and consciousness, the development and spread of digital technologies, but also how they will work within the legal system, what kind of connections these norms create and enter into, what place they will occupy in the legal system" (Khabriyeva & Chernogor, 2018). The formation of digital law should develop together with the entire legal system, without conflicting with it, and be its "augmented reality".

Internet Law

In European countries and the US, "Internet law" has already become an academic discipline. It first appeared in 1991 (Goldman, 2008), although most of the relevant legal regulation was created much later (Edwards & Waelde, 2009). Legal science gradually mastered a new sphere of public relations, which was being formed in the Internet space, along with the development of this space itself. Therefore, the most authoritative scientific publications on general issues of the digital challenge date back to the 1990s (Marsden, 2000). Of course, there have been more recent publications on individual digital innovations that appeared in the 2000s.

At the same time, various aspects of public relations and branches of the law were actively integrated from the physical environment into the digital one; these include intellectual property, telecommunications, privacy, cybercrime, and media content regulation. Despite its global nature, the Internet has a specific place of birth — the United States — so, initially, the legal research of Internet communications was based on American legal norms (Kahin & Nesson, 1997). Moreover, this trend is supported by the American scientific community, which occupies a leading position globally both in terms of the number of journals and the number of publications in the relevant field. Recently, the study of "Internet law" in the European Union has come to the forefront — Brussels has become a pioneer in legislation in many areas: combating cybercrime (cyberattacks, cybersecurity, Internet fraud, incitement to hostility and hatred, child pornography) (KjØrven, 2020); in the field of electronic commerce (Anagnostopoulou, 2018) and smart contracts (Seidel et al., 2020) with additional focus on consumer protection (Havu, 2017); in copyright (Colomo, 2017); in data protection (Zoboli, 2020); in banking (Langenbucher, 2020) and insurance services (Manes, 2020); and other such areas of the Internet. Of the most recent EU initiatives related to Internet law, it is worth noting the General Data

Protection Regulation (eng.), as well as a new Directive on Copyright in the Digital Single Market. When discussing the Directive on Copyright, the obvious contradictions between Internet corporations (sometimes called GAFA: Google, Amazon, Facebook, Apple) or activists (such as the Electronic Frontier Foundation[1]) fighting for free Internet, on the one hand, and copyright holders and content creators, on the other hand, became apparent. The Digital Markets Act and the Digital Services Act are at the first reading stage in the Council of the European Union, the significance of which, if approved and put into effect, is extremely difficult to overestimate. These regulations emerged due to the need to create a secure digital space in which the basic rights of users of digital services are protected and equal conditions are guaranteed to stimulate innovation, growth, and competitiveness.

Since the mid-1990s, the academic community has been extensively discussing the subject area of "Internet law" (Lessig, 1999). Many researchers believed that the digitalization of public relations would inevitably affect all branches of law, but would especially concern contract, antitrust, and constitutional law (Easterbrook, 1996; Sommer, 2000). Others have argued that Internet law is a short-term product generated by technological innovations and will inevitably be co-opted into existing legal institutions and branches of law (Larouche, 2008; Kerr, 2003).

Some authors consider Internet law as a branch of law, while others call it a branch of legislation; finally, Internet law can also be considered as a special kind of complex legal institution. From a doctrinal point of view, the authors agree that Internet law can be assigned its own separate place.

In Russia, the term "Internet law" did not catch on immediately. Rassolov, having made a decent review of the Russian literature, concluded that some scientists (Bachilo (2001a, 2001b, 2001c), Prosvirnin[2], Morozov (1999), Kopylov (1997, 2001)) do not specifically use the concept of Internet law, but instead — without giving clear and strict definitions of new categories and entities for the theory of law — simply pose and analyze some general methodological aspects of law and the Internet, legal problems of constructing the electronic environment and virtual space, and their functioning.

Other scientists (Rassolov[3], Soldatov (2002), Shagiyeva (2005)) differentiate the concept of "Internet law", although they do not disclose its essence and content. In doing so, they consider this concept as an independent research area in the structure of such branches as international private law and information law: i. e. as a kind of complex education within these branches.

In contrast, some researchers (in particular Yakushev[4]) advocate the development of Internet legislation, which will allow Internet relations to be regulated and will develop a new, vitally important terminology for the theory of law, namely: "Internet", "global network", "website", "domain address", "Internet relation", "subject of Internet relations", "information as a special object of civil law", "protection of intellectual property on the Internet", "judicial dispute on the Internet", and many others.

---

1 Electronic Frontier Foundation (eng. *EFF*) is a non-profit human rights organization founded in July 1990 in the United States to protect the rights enshrined in the Constitution and the Declaration of Independence in connection with the emergence of new communication technologies.

2 Prosvirnin, Y. G. (2002). Teoretiko-pravovyye aspekty informatizatsii v sovremennom Rossiyskom gosudarstve [Theoretical and legal aspects of informatization in the modern Russian state] [unpublished abstract of the doctoral dissertation]. Academy of Informatics, Economics and Law of the Moscow State Social University.

3 Rassolov, M. M. (2002). *Sbornik metodicheskikh materialov po kursam "Teoriya gosudarstva i prava" i "Problemy teorii gosudarstva i prava"* [*Collection of methodological materials on the courses "Theory of state and law" and "Problems of the theory of state and law"*]. Russian Law Academy of the Ministry of Justice of the Russian Federation; Rassolov, M. M. (2007). *Problemy teorii gosudarstva i prava* [*Problems of the theory of state and law*]. Yunii-Dana.

4 Yakushev, M. V. (2000). Internet i pravo: Novyye problemy, podkhody, resheniya [Internet and law: New problems, approaches, solutions]. *The Second All-Russian Conference "Law and the Internet: Theory and Practice"*. https://ifap.ru/pi/02/r03.htm

Finally, a number of authors (Gribanov (in Rassolov, 2009), Radchenko, Gorbunov[5] (2000), Naumov (2002), Goloskokov (2006)) discuss the further development of the legal theory in connection with the study of the global problems of virtual space (i. e., the Internet). For example, Radchenko and Gorbunov[6] distinguish the following elements of digital law: the right of digital state construction and public administration, copyright on digital entities, software law, the right of digital money, transactions, disputes, etc. Goloskokov wrote about network law, and Gribanov touched upon "the law of cybernetic space" (Rassolov, 2009).

Rassolov (2009) writes, in the conclusion to his literature review, that "at present, Internet law is a new independent area of legal science, and primarily information law".

Thus, in the Russian scientific discourse, a whole cloud of related concepts has formed around "Internet law": network law, information law, digital law, cybernetic space law. However, gradually "Internet law" has taken a dominant position. Several textbooks on Internet law[7] have been published.

Arkhipov, in his textbook "Internet Law", considers this term as conditional:

First of all, it refers to a set of legal norms aimed at regulating legal relations arising in connection with and about the Internet. Within the framework of the adopted methodological approach, it should be noted that this set of norms, in one way or another, should be aimed at directly or indirectly solving the systemic legal problems of Internet law. At the same time, on the one hand, this set of norms has a substantive unity due to this fact, on the other hand, there is no independent method of legal regulation in Internet law, although relations on the Internet from a broader point of view have a significant difference from all other public relations, since they can actually be regulated at the code level. Accordingly — since, according to the common point of view in the theory of law and the state, an independent branch of law is qualified simultaneously by the criteria of the subject and method, and Internet law has only a special subject unity — this set of legal norms cannot be considered an independent branch of law. At the same time, it should be noted that since the doctrine of Internet law (in comparison with other branches in the historical context) is generally only at the initial development stage, it is impossible to exclude changes in this scientific position in the future.[8]

On the other hand, Danilenkov notes in his textbook that Internet law has its own specific method:

The specificity of Internet law is that the above-mentioned scope of its norms — due to the extraterritoriality of individual segments of the Internet and the differences in the legal personalities of participants in network relations given the subordination of their personal status or corporate legal capacity to different jurisdictions — sometimes become entwined in a real tangle of contradictions and problems. All this sometimes requires the use of special methods and methodologies to determine the jurisdiction of the dispute, as well as the applicable law in order to resolve legal conflicts and disputes, in particular based on the principle of close connection (the concept of "genuine link") between the Internet relationship (complicated by its foreign element) with the law of the relevant country, while observing the requirements of international reciprocity, politeness, etc. (Danilenkov, 2014).

Thus, the peculiarity of the Internet law method lies in the specifics of resolving issues of conflict of jurisdictions and conflict of laws in the Internet space.

---

5 Radchenko, M. Y., & Gorbunov, V. P. (2000). Digital law of the future [Digital law of the future]. *The Second All-Russian Conference "Law and the Internet: Theory and Practice"*. https://ifap.ru/pi/02/r03.htm

6 Radchenko & Gorbunov, 2000.

7 Arkhipov, V. V. (2016). *Internet-pravo: Uchebnik i praktikum dlya bakalavriata i magistratury* [*Internet Law: A textbook and a practical course for bachelor's and master's degrees*]. Yurayt Publishing House.

8 Arkhipov, 2016.

Digital Law

Unlike Internet law, Russian digital law is only beginning to be understood and established as a tool for legal regulation, as well as for laying the foundations for the digital economy's development. In 2018, the national project "Digital Economy" was launched in Russia, which will end in 2024. During this time, it is intended to achieve the following goals:

1. To increase domestic spending on the development of the digital economy from all sources (as a share of GDP) by at least 3 times compared to 2017.
2. To create a stable and secure information and telecommunications infrastructure for transmitting, processing, and storing large amounts of data, accessible to all organizations and households.
3. To enable state bodies, local governments, and Russia-based organizations to use mainly domestic software.[9]

This national project includes six others: "Digital environment regulation"; "Information Infrastructure"; "Personnel for the digital economy"; "Information Security"; "Digital Technologies"; "Digital Public Administration". The federal project "Digital Environment regulation" essentially forms the Russian digital law.

The passport[10] of this project outlines an idea of the main directions of digital law development. There are nine such directions:

1. Creating legal preconditions for a single digital environment of trust.
2. Creating legal preconditions for electronic civil turnover.
3. Ensuring a facilitating legal environment for collecting, storing, and processing data.
4. Ensuring legal conditions for introducing and using innovative technologies in the financial market.
5. Creating regulatory incentives for developing the digital economy.
6. Forming legal conditions in the field of legal proceedings and notaries in connection with the development of the digital economy.
7. Regulating the business-state digital interaction.
8. Comprehensively developing the legislation regulating relations in the field of the digital economy, as well as creating a mechanism for managing changes and competencies (knowledge) in the field of digital economy regulation.
9. "Other measures", a section which mentions the development of the digital economy in the EAEU.

The "Concept of Complex Legal Regulation of Relations Arising in Connection with the Digital Economy Development" (hereinafter referred to as the Concept), proposed by the Institute of Legislation and Comparative Law under the Government of the Russian Federation, provides an overview of the current state of legal regulation experienced by the digital economy all over the world. The regulation of international digital technologies originates in the documents of international

---

[9] The Russian Government. (2019, February 11). *Opublikovan passport natsional'noy programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii"* [*The passport of the national program "Digital Economy of the Russian Federation" has been published*] [Infographic. Information materials about the national program "Digital Economy of the Russian Federation"]. http://government.ru/info/35568/

[10] The Russian Government. (2019, February 11). *Opublikovan passport natsional'noy programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii"* [*The passport of the national program "Digital Economy of the Russian Federation" has been published*] [Document. Passport of the national program "Digital Economy of the Russian Federation"]. http://government.ru/info/35568/

organizations: these include the G20 Initiative for Development and Cooperation in the Field of Digital Economy 2016 as well as the OECD Cancun Declaration on the Digital Economy 2016, amongst others. The provisions of these documents were developed and specified by many acts of the Group of Twenty, the Financial Stability Board, the OECD, the FATF, the International Monetary Fund, the Bank for International Settlements, and the International Organization of Securities Commissions, as well as other global standard-setters and European regulators.[11]

The Concept identifies the following four key approaches to the legal regulation of the digital economy at the national level: legislative, subordinate, national strategic, and regional strategic.

The Concept analyzes these models of legally regulating the digital economy, highlighting the strengths and weaknesses of each of them.

The *legislative regulation* of the digital economy has certain advantages: the regulatory consolidation of the elements of the digital economy allows them to hold an official status at the legislative level. As part of a comprehensive law, the elements of the digital economy are integrated into a hierarchical system of regulatory legal acts, becoming the next step after the basic law of the state.

This model also has disadvantages, the main one being related to the order of change. In order to change the text of the law, the necessary procedure for making such changes must be followed. These changes vary from one state to another, but this process is quite time-consuming and lengthy in absolutely all states. The next biggest drawback is that the elements of the digital economy are developing non-linearly and extremely rapidly, therefore the authorities may not have time to adapt the legislative system to the latest changes and, as a result, regulatory gaps may appear.

The *bylaw regulation of the digital economy* has the following advantages: an operational procedure for adopting regulations and great opportunities for adapting regulation to scientific and technological progress.

This model also has some disadvantages. For example, when placing the digital economy regulation under the aegis of the executive authorities and excluding the legislature from the law-making process, there is a risk of the people's opinion not being considered in completeness.

The *national strategic approach* is the most balanced. It has the following advantages: procedure for adoption and change, thus being the most rapid to adapt; long-term perspective (as a rule); and it can consider public opinion, as well as that of public organizations, the business community, and government representatives.

Despite this, the approach has one significant drawback — in the absence of an imperative, problems with its implementation may arise, especially if the strategy is designed for the long term. Competent, complete, and comprehensive implementation of the strategy requires the coordinated and harmonious approach of several actors involved. Failure of one "link" can jeopardize the entire strategy.

The *regional strategic* model has proven itself well in some federal states, but it can only be relied on in conditions of more or less the same position of the subjects of the federation (both in the organizational, legal sense and the economic sense). In other words, such a model can be successfully implemented in symmetric federations, in which all subjects are in the same position and have approximately equal opportunities. On the other hand, in asymmetric federations, it will most likely not be able to function normally due to the different capabilities of the subjects (states, lands, territories, cantons, provinces, etc.) of the federation.

[11] The international agenda is also covered in scientific works. Russian and foreign researchers are seriously discussing the prospects for the use of digital technologies and the development of digital law at the level of interstate associations to more effectively develop international cooperation, for example, in the field of criminal prosecution (Nikitin & Marius, 2020).

The Concept notes that the Russian Federation is moving towards building such a hybrid model, adding elements of each of the main models considered. No matter what, though, one of the models included in it will dominate. Russia is likely to follow the path of a nationwide strategic model, of which Estonia is a prime example. Its attractiveness is explained not only by the balance already noted but also by the fact that it is aimed at regulating the digital economy 2.0, which does not suggest direct human involvement in the system.

***

Dear readers!

"Digital law" as a legal reflection of the digital economy is still in its infancy. The rapid development of public relations and the increasing complexity of trade pose several new questions to the international scientific community; answering these using the achievements of legal science of the 19th–20th centuries is not always possible. Instead it requires a modern conceptual framework, as well as a potential rethinking of traditional legal categories.

Digital Law Journal has been an important discussion platform for two years already. The current state of existing digital technologies, specific features, and the prospects for their full-scale implementation in the regulatory and legal field are analyzed in this journal from both scientific and practical points of view.

The magazine has achieved a lot during the years of its existence. Our editorial board includes exceptional scientists alongside representatives of scientific schools both in Russia and internationally, all of whom deal with the problems of digital law. The journal publishes the works of the authors whose research sets the tone for the modern "digital" debate. The legal regulation of smart contracts and telemedicine, the creation of "regulatory sandboxes", the place of artificial intelligence in the structure of legal relations, labor market digitalization, and the peculiarities of human rights, competition, and the tax system in the digital age are just some of the issues that have been discussed in our journal. Each submitted manuscript is invariably subject to a double-blind peer review, conducted anonymously by recognized experts in their field of research. The journal is published with a steady frequency.

Of course, all this would not have been possible without you, thoughtful and patient readers who are interested in the problems of digital law, methodological and substantive changes in traditional branches of law that are emerging in the era of the digital economy. Your interest in our project contributes to its continuous development, improving the quality of publications and attracting new readers, authors, and experts.

We are pleased to present to your attention the first issue of the second volume and hope that 2021 will bring only success to our common cause!

Kind regards,
Editor-in-Chief
Dr. Maxim Inozemtsev

References:

1. Anagnostopoulou, D. (2018). The withdrawal of the common European sales law proposal and the European commission proposal on certain aspects concerning contracts for the online and other distance sales of goods. In M. Heidemann, & J. Lee (Eds.), *The future of the commercial contract in scholarship and law reform: European and comparative perspectives* (pp. 127–163). Springer, Cham. https://doi.org/10.1007/978-3-319-95969-6_6
2. Bachilo, I. L. (2001a). Aktual'nyye problemy informatsionnogo prava. [Actual problems of information law]. *Nauchno-tekhnicheskaya informatsiya. Seriya 1: Organizatsiya i metodika informatsionnoy raboty*, *9*, 3–8.
3. Bachilo, I. L. (2001b). *Informatsionnoye pravo* [Information law]. Yurinformtsentr.
4. Bachilo, I. L. (2001c). Informatsionnoye pravo. Rol' i mesto v sisteme prava Rossiyskoy Federatsii [Information law. Role and place in the legal system of the Russian Federation]. *Gosudarstvo i Pravo*, *2*, 5–14.
5. Colomo, P. I. (2017). Copyright licensing and the EU digital single market strategy. In R. Blair, & D. Sokol (Eds.), *The Cambridge handbook of antitrust, intellectual property, and High Tech (Cambridge law handbooks*, pp. 339–357). Cambridge University Press. https://doi.org/10.1017/9781316671313.018
6. Danilenkov, A. V. (2014). *Internet-Pravo* [Internet law]. Yustitsinform.
7. Easterbrook, F. H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum*, *1996*, Article 7. https://chicagounbound.uchicago.edu/uclf/vol1996/iss1/7
8. Edwards, L., & Waelde, C. (Eds.). (2009). *Law and the Internet*. Bloomsbury Publishing.
9. Goldman, E. (2008). Teaching cyberlaw. *Saint Louis University Law Journal*, *52*(3), 749–764.
10. Goloskokov, L. V. (2006). *Teoriya setevogo prava* (A. V. Malko, ed.) [Network law theory]. Izd-vo R. Aslanova.
11. Havu, K. (2017). The EU digital single market from a consumer standpoint: How do promises meet means? *Contemporary Readings in Law and Social Justice, 9*(2), 146–183. https://doi.org/10.22381/CRLSJ9220179
12. Kahin, B., & Nesson, C. (Eds.). (1997). *Borders in cyberspace: Information policy and the global information infrastructure*. MIT Press.
13. Kerr, O. S. (2003). The problem of perspective in Internet law. *Georgetown Law Journal*, *91*, 357-405.
14. Khabriyeva, T. Y., & Chernogor, N. N. (2018). Pravo v usloviyakh tsifrovoy real'nosti [Law in the context of digital reality]. *Zhurnal Rossiyskogo Prava*, *1*, 85–102. https://doi.org/10.12737/art_2018_1_7
15. KjØrven, M. E. (2020). Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe. *European Business Law Review*, *31*(1), 77–109. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020004
16. Kopylov, V. A. (1997). *Informatsionnoye pravo* [Information law]. Yurist.
17. Kopylov, V. A. (2001). Internet i pravo [Internet and law]. *Nauchno-Tekhnicheskaya Informatsiya. Seriya 1: Organizatsiya i Metodika Informatsionnoy Raboty*, (9), 8.
18. Langenbucher, K. (2020). Responsible A.I.-Based credit scoring — A legal framework. *European Business Law Review*, *31*(4), 527–571. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.4/EULR2020022
19. Larouche, P. (2008). On the future of information law as a specific field of law (Discussion Paper No. 2008–020). Tilburg University: Tilburg Law and Economics Center.
20. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, *113*(2), 501–549. https://doi.org/10.2307/1342331
21. Manes, P. (2020). Legal challenges in the realm of InsurTech. *European Business Law Review*, *31*(1), 129–168. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020006
22. Marsden, C. T. (Ed.). (2000). *Regulating the global information society* (Vol. 2). Psychology Press.

23. Morozov, A. V. (1999). *Sistema pravovoy informatizatsii Minyusta Rossii* [The system of legal informatization of the Ministry of Justice of Russia]. Triumf.
24. Naumov, V. B. (2002). *Pravo i Internet: Ocherki teorii i praktiki* [Law and the Internet: Essays on theory and practice]. Knizhnyy Dom "Universitet".
25. Nikitin, E., & Marius, M. C. (2020). Unified digital law enforcement environment — Necessity and prospects for creation in the "BRICS countries". *BRICS Law Journal*, *7*(2), 66–93. https://doi.org/10.21684/2412-2343-2020-7-2-66-93
26. Rassolov, I. M. (2009). *Pravo i Internet. Teoreticheskiye problemy* (2nd ed.) [Law and the Internet. Theoretical Problems]. Norma.
27. Seidel, E., Horsch, A., & Eickstädt, A. (2020). Potentials and limitations of smart contracts: A primer from an economic point of view. *European Business Law Review*, *31*(1), 169–183. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020007
28. Shagiyeva, R. V. (2005). *Kontseptsiya pravovoy deyatel'nosti v sovremennom obshchestve* [The concept of legal activity in modern society]. Izdatel'stvo Kazanskogo Universiteta.
29. Soldatov, A. S. (2002). *Pravo kak instrument sotsial'nogo upravleniya* [Law as an instrument of social management]. Yurist.
30. Sommer, J. H. (2000). Against cyberlaw. *Berkeley Technology Law Journal*, *15*(3), 1145–1232.
31. Zoboli, L. (2020). Fueling the European digital economy: A regulatory assessment of B2B data sharing. *European Business Law Review*, *31*(4), 663–692. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.4/EULR2020026

Information about the author:

Maxim I. Inozemtsev — Ph.D. in Law, Associate Professor, Department of Private International and Civil Law, MGIMO-University, Editor-in-Chief, Digital Law Journal, Moscow, Russia.
inozemtsev@inno.mgimo.ru
ORCID 0000-0003-1845-1363

Сведения об авторе:

Иноземцев М. И. — кандидат юридических наук, доцент кафедры международного частного и гражданского права им. С. Н. Лебедева МГИМО МИД России, главный редактор журнала «Цифровое право» (Digital Law Journal), Москва, Россия.
inozemtsev@inno.mgimo.ru
ORCID 0000-0003-1845-1363

https://doi.org/10.38044/2686-9136-2021-2-1-8-28

ОТ РЕДАКЦИИ

ЦИФРОВОЕ ПРАВО: В ПОИСКАХ ОПРЕДЕЛЕННОСТИ

М.И. Иноземцев

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

Аннотация

В статье рассматривается вопрос развития цифрового права как инструмента нормативного регулирования цифровой экономики. Доказывается, что пока более устоявшимся, нежели понятие «цифровое право», в академической среде является понятие «интернет-право». Именно в такой форме правовая сфера отвечает на вызовы цифровой революции и является отражением цифровой экономики. До сих пор не утихли споры, можно ли рассматривать «интернет-право» в качестве отдельной отрасли права или отрасли законодательства. Тем не менее это несомненно самостоятельная академическая дисциплина, учебники по которой издаются уже и в России. Необходимость развития цифровой экономики остро стоит и перед Россией, в этих целях в 2018 г. был принят национальный проект «Цифровая экономика РФ». Нормативное обеспечение реализации данного проекта формирует основу цифрового права в России. При этом учитывается обширный опыт нормативного регулирования цифровой экономики в странах ближнего и дальнего зарубежья. Особенно привлекательной выглядит общенациональная стратегическая модель, которая предполагает наиболее оперативный порядок принятия изменений, следовательно, и адаптации цифрового законодательства, нацелена на долгосрочную перспективу, позволяет учитывать мнение населения, общественных организаций, бизнес-сообщества, представителей власти. Помимо зарубежного опыта нормативного регулирования цифровой экономики необходимо также использовать наработки отечественной и зарубежной правовой науки.

Ключевые слова

цифровое право, интернет-право, цифровая экономика, промышленная революция, национальная программа

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Иноземцев, М. И. (2021). Цифровое право: в поисках определенности. *Цифровое право, 2*(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Поступила: 21.01.2021; принята в печать: 15.02.2021; опубликована 31.03.2021

EDITORIAL

DIGITAL LAW: THE PURSUIT OF CERTAINTY

Maxim I. Inozemtsev

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

Abstract

The article deals with the development of digital law as an instrument for regulating the digital economy. It is proved that, within the academic environment, the concept of "Internet law" is still more well-established than the concept of "digital law". It is in this manner that the legal sphere responds to the challenges of the digital revolution and reflects the digital economy. The debate as to whether "Internet law" can be considered either as a separate branch of law or as a branch of legislation has not yet subsided. Nevertheless, "Internet law" is undoubtedly an independent academic discipline, textbooks on which are published in Russia. However, Russia needs to develop a digital economy; this is why the national project "Digital Economy of the Russian Federation" was adopted in 2018, regulatory support for which forms the basis of digital law in Russia. At the same time, the extensive experience of digital economy regulation in both its neighbouring countries and beyond is taken into account. Especially attractive is the national strategic model, which assumes the most rapid procedure for adopting changes and consequently adapting digital legislation, is aimed at the long-term perspective, and lets popular opinion — as well as the opinions of public organizations, the business community, and government representatives — be taken into account. In addition to foreign experience in regulating the digital economy, we should also use the best practices of domestic and foreign legal science.

Keywords

digital law, Internet law, digital economy, industrial revolution, national program

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Inozemtsev, M. I. (2021). Digital law: The pursuit of certainty. *Digital Law Journal, 2*(1), 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Submitted: 21 Jan. 2021, accepted: 15 Feb. 2021, published: 31 Mar. 2021

Постановка вопроса

Становление цифровой экономики и информационного общества неизбежно требует развития «цифрового права» как инструмента регулирования общественных отношений online, а также общественных отношений по поводу цифровых объектов в форме данных и знаний. Специфика цифровой сферы зачастую не позволяет автоматически применять к ней существующие нормы и институты права. При этом ответ на вопрос о том, как адаптировать существующие правовые нормы к цифровой среде, неочевиден и требует научной рефлексии международного сообщества правоведов.

Задача осложняется тем, что современные общественные отношения зачастую носят гибридный характер — они разворачиваются одновременно в двух сферах: физической и цифровой. Эти сферы глубоко проникли друг в друга, но не взаимозаменяемы. Цифровое пространство скорее дополняет физическое, формируя «дополненную реальность». Однако при описании их взаимодействия у исследователей часто возникает соблазн видеть игру с нулевой суммой: либо объявлять, что «цифра» полностью изменила общественные отношения, либо что влияние это, прежде всего, количественное, а не качественное, притом что цифровая сфера сама форматируется общественными отношениями, сложившимися до ее появления. Попытки нейтрально разобраться в отношениях между этими двумя сферами и влиянием, которое это взаимодействие оказывает на различные стороны общественных отношений, встречаются крайне редко.

Праву необходимо учитывать этот гибрид, но регулировать его не как две отдельные сферы, существующие каждая в своей логике, а как системную целостность, формируемую общественными отношениями. Так, Т. Я. Хабриева отмечает, что «констатировать появление своего рода «кросс-отраслевых» юридических норм, обеспечивающих «перепрошивку» права под цели и задачи цифровой экономики, явно недостаточно. Важно осмыслить не только то, как и с каким эффектом они будут воздействовать на общественные отношения, волю и сознание людей, развитие и распространение цифровых технологий, но и как поведут себя внутри системы права, какого рода связи эти нормы создают и в какие вступают, какое место они займут в системе права» (Khabriyeva & Chernogor, 2018). Формирование цифрового права должно развиваться вместе со всей системой права, не вступая с ней в противоречия, и быть ее «дополненной реальностью».

Интернет-право

На Западе «интернет-право» уже сформировалось как академическая дисциплина. Ее начало можно датировать приблизительно 1991 годом (Goldman, 2008), хотя большая часть соответствующего правового регулирования сформировалась существенно позже (Edwards & Waelde, 2009). Правоведение постепенно осваивало новую сферу общественных отношений, формирующуюся в интернет-пространстве, параллельно с развитием самого этого пространства. Поэтому большинство наиболее авторитетных научных публикаций по общим вопросам цифрового вызова относятся к 1990-м годам (Marsden, 2000). Конечно, есть и более свежие публикации по отдельным цифровым инновациям, появившимся уже в 2000-х годах.

В это же время происходила активная интеграция различных аспектов общественных отношений и отраслей права из физической среды в цифровую: интеллектуальная собственность, телекоммуникации, конфиденциальность, киберпреступность, регулирование медиаконтента. Несмотря на свою глобальную природу, у Интернета есть конкретное место рождения — США, поэтому изначально предметом правовых исследований интернет-коммуникаций были правовые нормы именно этой страны (Kahin & Nesson, 1997). Причем эта тенденция усугубляется активностью самого американского научного сообщества, которое и по количеству журналов, и по количеству публикаций в соответствующей области занимает лидирующие позиции в мире. В последнее время на передний план выходит изучение «интернет-права» в Европейском Союзе — Брюссель стал пионером в законодательстве во многих областях: борьбы с киберпреступностью (кибератаки, кибербезопасность, интернет-мошенничество, призывы к вражде и ненависти, детская порнография) (Kjørven, 2020), в сфере электронной торговли (Anagnostopoulou,

2018) и смарт-контрактов (Seidel et al., 2020) (с акцентом на защите прав потребителей) (Havu, 2017), в авторском праве (Colomo, 2017), защите данных (Zoboli, 2020), банковских (Langenbucher, 2020) и страховых услуг (Manes, 2020) и т. п. Из самых новых инициатив ЕС, связанных с интернет-правом, стоит отметить «Общий регламент по защите данных» (англ. *General Data Protection Regulation*), а также новую «Директиву об авторском праве на Едином цифровом рынке». При обсуждении Директивы об авторском праве стали очевидны явные противоречия между гигантскими интернет-корпорациями (иногда называемыми GAFA: Google, Amazon, Facebook, Apple), активистами, борющимися за свободу интернета (таких, как Фонд электронных рубежей[1]), с одной стороны, и правообладателями авторских прав и создателями контента, с другой стороны. На стадии первого чтения в Совете Европейского Союза находятся «Акт о цифровых рынках» и «Акт о цифровых услугах», значение которых в случае их одобрения и введения в действие переоценить крайне сложно. Разработка указанных регламентов связана с необходимостью создания безопасного цифрового пространства, в котором обеспечивается защита основных прав пользователей цифровых услуг и гарантируются равные условия для стимулирования инноваций, роста и конкурентоспособности.

С середины 1990-х годов в научной среде велись широкие дискуссии о предметной области «интернет-права» (Lessig, 1999). Многие исследователи полагали, что информатизация общественных отношений неизбежно затрагивает все отрасли права, но особенно касается договорного, антимонопольного и конституционного права (Easterbrook, 1996; Sommer, 2000). Другие утверждают, что интернет-право — это кратковременный продукт, порожденный технологическими инновациями, который будет в последствии неизбежно кооптирован в существующие правовые институты и отрасли права (Larouche, 2008; Kerr, 2003).

Таким образом, некоторые авторы рассматривают интернет-право как отрасль права, другие как отрасль законодательства, наконец, интернет-право может рассматриваться как особая разновидность комплексного правового института. Авторы при этом сходятся во мнении о том, что за интернет-правом доктринально может быть закреплено отдельное место.

В России термин «интернет-право» прижился не сразу. И. М. Рассолов, сделав достойный обзор российской литературы, пришел к выводу, что одни ученые (И. Л. Бачило (Bachilo, 2001a; 2001b; 2001c), Ю. Г. Просвирнин[2], А. В. Морозов (Morozov, 1999), В. А. Копылов (Kopylov, 1997; 2001)) специально не оперируют понятием интернет-права, а просто ставят и анализируют некоторые общеметодологические аспекты права и Интернета, правовые проблемы построения и функционирования электронной среды и виртуального пространства, не давая четких и строгих определений новым для теории права категориям и сущностям.

Другие ученые (М. М. Рассолов[3], А. С. Солдатов (Soldatov, 2002), Р. В. Шагиева (Shagiyeva, 2005)) в ходе своих научных изысканий выделяют понятие «интернет-право», правда, не раскрывая его сущность и содержание. При этом они рассматривают данное понятие как самостоятельное

---

[1] Фонд Электронных Рубежей (англ. *Electronic Frontier Foundation, EFF*) — основанная в июле 1990 в США некоммерческая правозащитная организация с целью защиты заложенных в Конституции и Декларации независимости прав в связи с появлением новых технологий связи.

[2] Просвирнин, Ю. Г. (2002). Теоретико-правовые аспекты информатизации в современном Российском государстве [неопубликованный автореферат докторской диссертации]. Академия информатики, экономики и права Московского государственного социального университета.

[3] Рассолов, М. М. (2002). *Сборник методических материалов по курсам «Теория государства и права» и «Проблемы теории государства и права»*. Российская правовая академия МЮ РФ; Рассолов, М. М. (2007). *Проблемы теории государства и права*. Юнити-Дана.

направление в структуре таких отраслей как международное частное право и информационное право, т. е. как некое комплексное образование внутри этих отраслей.

Напротив, некоторые исследователи (в частности, М. В. Якушев[4]) ратуют за развитие интернет-законодательства, которое позволит урегулировать интернет-отношения и выработать для теории права новую, столь важную терминологию, а именно: «Интернет», «глобальная сеть», «сайт», «доменный адрес», «интернет-отношение», «субъект интернет-отношений», «информация как особый объект гражданского права», «охрана интеллектуальной собственности в Сети», «судебный спор в Интернете» и многие другие.

И наконец, ряд авторов (Д. В. Грибанов, М. Ю. Радченко, В. П. Горбунов[5], В. Б. Наумов (Naumov, 2002), Л. В. Голоскоков (Goloskokov, 2006)) рассуждают о дальнейшем развитии теории права в связи с исследованием всемирных проблем виртуального пространства (т. е. Интернета). К примеру, М. Ю. Радченко и В. П. Горбунов[6] в качестве элементов цифрового права выделяют: право цифрового государственного строительства и государственного управления, авторское право на цифровые сущности, программное право, право цифровых денег, операций, споров и т. д. Л. В. Голоскоков рассуждает о сетевом праве, а Д. В. Грибанов – о «праве кибернетического пространства» (Rassolov, 2009).

И. М. Рассолов, отталкиваясь от проведенного обзора, полагает, что «в настоящее время интернет-право — это новое самостоятельное направление юридической науки, и прежде всего информационного права» (Rassolov, 2009).

Таким образом, в российском научном дискурсе сформировалось целое облако смежных понятий вокруг «интернет-права»: сетевое право, информационное право, цифровое право, право кибернетического пространства. Однако постепенно «интернет-право» заняло доминирующие позиции. Было издано несколько учебников по «интернет-праву»[7].

В. В. Архипов в своем учебнике «Интернет-право» одноименный термин рассматривает как условный. «Прежде всего, он обозначает совокупность правовых норм, нацеленных на регулирование правовых отношений, возникающих в связи и по поводу сети Интернет. В рамках принятого методологического подхода следует отметить, что данная совокупность норм, так или иначе, должна быть нацелена на то, чтобы прямо или косвенно разрешить системные правовые проблемы интернет-права. При этом, с одной стороны, у данной совокупности норм есть предметное единство, обусловленное указанным фактом, с другой — в интернет-праве отсутствует самостоятельный метод именно правового регулирования, хотя отношения в сети Интернет с более широкой точки зрения обладают существенным отличием от всех других общественных отношений, поскольку могут фактически регулироваться на уровне кода. Соответственно, поскольку согласно распространенной в теории права и государства точке зрения самостоятельная отрасль права квалифицируется одновременно по критериям предмета и метода, а интернет-право обладает лишь особенным предметным единством, данную совокупность правовых норм нельзя считать самостоятельной отраслью права. В то же время следует отметить, что в силу того, что доктрина интернет-права по сравнению с другими отраслями в историческом контексте находится

[4] Якушев, М. В. (2000). Интернет и право: новые проблемы, подходы, решения. *Вторая Всероссийская конференция «Право и Интернет: теория и практика»*. https://ifap.ru/pi/02/r03.htm

[5] Радченко, М. Ю., Горбунов, В. П. (2000). Цифровое право будущего. *Вторая Всероссийская конференция «Право и Интернет: теория и практика»*. https://ifap.ru/pi/02/r03.htm

[6] Радченко, Горбунов, 2000.

[7] Архипов, В. В. (2016). *Интернет-право: учебник и практикум для бакалавриата и магистратуры*. Издательство Юрайт.

в целом лишь на начальном этапе развития, нельзя исключить изменения данной научной позиции в дальнейшем»[8]. Напротив, А. В. Даниленков в своем учебнике отмечает наличие у интернет-права своего специфического метода. «Специфика интернет-права состоит в том, что указанные выше сферы действия его норм в силу экстерриториальности отдельных сегментов сетевого пространства Интернета и разной правосубъектности участников сетевых отношений в виду подчинения их личного статуса или корпоративной правоспособности различным юрисдикциям иногда сплетаются в настоящий клубок коллизионных противоречий и проблем. Все это подчас требует применения специальных способов и методов для определения подсудности спора, а также применимого права с целью разрешения юридических конфликтов и споров, в частности, на основе принципа тесной связи (концепция "*genuine link*") между интернет-отношением, осложненным иностранным элементом, с правом соответствующей страны при соблюдении требований международной взаимности, вежливости и т. д.» (Danilenkov, 2014). Таким образом, особенность метода интернет-права заключается в специфике решения в интернет пространстве вопросов коллизии юрисдикций и коллизии законов.

Цифровое право

В отличие от интернет-права, цифровое право в России только начинает пониматься и формироваться как инструмент правового регулирования и создания условий для развития цифровой экономики. В 2018 году в России был запущен национальный проект «Цифровая экономика», который продлится до 2024 года. За это время планируется достичь следующих целей:

1. Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в ВВП) не менее чем в 3 раза по сравнению с 2017 г.
2. Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств.
3. Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями[9].

В указанный национальный проект входят шесть других: «Нормативное регулирование цифровой среды»; «Информационная инфраструктура»; «Кадры для цифровой экономики»; «Информационная безопасность»; «Цифровые технологии»; «Цифровое государственное управление». Реализация федерального проекта «Нормативное регулирование цифровой среды» по сути формирует российское цифровое право.

Из паспорта[10] этого проекта можно составить представление об основных направлениях развития цифрового права. Таких направлений девять:

1. Создание правовых условий для формирования единой цифровой среды доверия.
2. Создание правовых условий для формирования электронного гражданского оборота.

---

[8] Архипов, 2016.

[9] Правительство России. (2019, февраль 11). *Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации»* [Инфографика. Информационные материалы о национальной программе «Цифровая экономика Российской Федерации»]. http://government.ru/info/35568/

[10] Правительство России. (2019, февраль 11). *Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации»* [Документ. Паспорт национальной программы «Цифровая экономика Российской Федерации»]. http://government.ru/info/35568/

3. Обеспечение благоприятных правовых условий для сбора, хранения и обработки данных.
4. Обеспечение правовых условий для внедрения и использования инновационных технологий на финансовом рынке.
5. Нормативное стимулирование развития цифровой экономики.
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.
8. Комплексное развитие законодательства, регулирующего отношения в области цифровой экономики, а также создание механизма управления изменениями и компетенциями (знаниями) в области регулирования цифровой экономики.
9. В разделе «иные меры» упоминается развитие цифровой экономики в ЕАЭС.

В «Концепции комплексного правового регулирования отношений, возникающих в связи с развитием цифровой экономики» (далее — Концепция), предложенной Институтом законодательства и сравнительного правоведения при правительстве РФ, дан обзор существующего положения дел в мире по правовому регулированию цифровой экономики. Международное регулирование цифровых технологий берет начало в документах международных организаций: Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики 2016 года, Канкунская декларации ОЭСР о цифровой экономике 2016 года и т. д. В дальнейшем положения указанных документов были развиты и конкретизированы множеством актов со стороны «Группы двадцати», Совета по финансовой стабильности, ОЭСР, ФАТФ, Международного валютного фонда, Банка международных расчетов, Международной организации комиссий по ценным бумагам, а также иных глобальных стандарт-сеттеров и европейских регуляторов[11].

На национальном уровне Концепция выделяет следующие четыре ключевых подхода к правовому регулированию цифровой экономики: законодательный, подзаконный, общенациональный стратегический, региональный стратегический.

В Концепции проводится анализ этих моделей правового регулирования цифровой экономики с выделением сильных и слабых сторон каждой из них.

Подход *законодательного регулирования* цифровой экономики имеет отдельные преимущества: нормативное закрепление элементов цифровой экономики позволяет придать им официальный статус на законодательном уровне. Будучи частью комплексного закона элементы цифровой экономики встраиваются в иерархичную систему нормативных правовых актов, оказываясь следующей ступенью после основного закона государства.

Рассматриваемая модель также имеет недостатки, главный из которых связан с порядком изменения. Для того чтобы изменить текст закона, должен быть соблюден необходимый порядок внесения изменений, которые варьируются от одного государства к другому, однако абсолютно во всех государствах этот процесс достаточно трудоемкий и длительный. Следующий недостаток сопряжен с тем, что элементы цифровой экономики развиваются нелинейно и крайне стремительно, следовательно, органы власти могут не успевать адаптировать законодательную систему к последним изменениям, в результате чего образуются бреши в регулировании.

[11] Международной повестке уделяют внимание и в научной литературе. Российские и зарубежные исследователи всерьез обсуждают перспективы использования цифровых технологий и развития цифрового права на уровне межгосударственных объединений для более эффективной реализации международного сотрудничества, например, в области уголовного преследования (Nikitin & Marius, 2020).

Подход *подзаконного регулирования цифровой экономики* имеет следующие преимущества: оперативный порядок принятия нормативных актов и большие возможности адаптации регулирования к научно-техническому прогрессу.

В то же время такая модель имеет и недостатки. Так, отдав регулирование цифровой экономики под эгиду органов исполнительной власти и исключив легислатуру из процесса законотворчества, возникает риск неполного учета мнения граждан того государства, в котором принимаются решения относительно цифровой экономики.

Общенациональный стратегический подход является наиболее сбалансированным. Он имеет следующие преимущества: наиболее оперативный порядок принятия и изменения, следовательно, и адаптации; долгосрочная (как правило) перспектива; есть возможность учитывать мнение населения, общественных организаций, бизнес-сообщества, представителей власти.

Несмотря на это подход имеет один существенный недостаток — в отсутствие императивности могут возникнуть проблемы с его реализацией, особенно если стратегия рассчитана на долгосрочную перспективу. Грамотная, полная и всеобъемлющая реализация стратегии требует слаженной и гармоничной работы нескольких субъектов, задействованных в реализации. Отказ одного «звена системы» может поставить под угрозу реализацию всей стратегии в целом.

Региональная стратегическая модель хорошо себя зарекомендовала в некоторых федеративных государствах, однако на нее можно полагаться только в условиях более-менее одинакового положения субъектов федерации (как в организационно-правовом, так и в экономическом смысле). Говоря иначе, подобная модель будет успешно реализована в симметричных федерациях, где все субъекты находятся в одном положении и имеют примерно равные возможности реализации. В ассиметричных федерациях она, скорее всего, не сможет функционировать нормально из-за различных возможностей субъектов (штатов, земель, территорий, кантонов, провинций и т. д.) федерации.

В Концепции отмечается, что Российская Федерация движется по пути построения подобной гибридной модели, пополняясь элементами каждой из рассмотренных основных моделей. Тем не менее, в любой гибридной версии одна из входящих в нее моделей будет доминировать. Россия, скорее всего, пойдет по пути общенациональной стратегической модели, ярким примером которой является Эстония. Ее привлекательность объясняется не только уже отмеченной сбалансированностью, но и тем обстоятельством, что она направлена на регулирование цифровой экономики версии 2.0, не предполагающей непосредственного участия человека в функционировании системы.

***

Уважаемые читатели!

«Цифровое право» как правовое отражение цифровой экономики пока только зарождается. Бурное развитие общественных отношений и усложняющийся торговый оборот ставят перед мировым научным сообществом ряд новых вопросов, ответить на которые не всегда представляется возможным, используя достижения правовой науки XIX–XX вв. Требуется разработка современного понятийного аппарата, и, вероятно, переосмысление традиционных правовых категорий.

Журнал «Цифровое право» (Digital Law Journal) уже второй год является важной дискуссионной площадкой, где в научно-практической плоскости осмысляется современное состояние имеющихся цифровых технологий, специфические особенности и перспективы их полномасштабного внедрения в нормативно-правовое поле.

За год своего существования журналу удалось достичь многого. В нашу редакционную коллегию вошли исключительные ученые, представители российской и зарубежных научных школ, разрабатывающие проблематику цифрового права. В журнале публикуются авторы, чьи исследования задают тон современной «цифровой» дискуссии. Проблемы правового регулирования смарт-контрактов и телемедицины, создания «регулятивных песочниц», места искусственного интеллекта в структуре правоотношения, цифровизации рынка труда, а также особенности прав человека, конкуренции и налоговой системы в цифровую эпоху — лишь часть тех вопросов, которые были рассмотрены на страницах нашего журнала. Каждая присланная рукопись неизменно проходит процедуру двойного слепого рецензирования, анонимно осуществляемого признанными экспертами в своей области исследования. Номера журнала публикуются с устойчивой периодичностью.

Безусловно, все это было бы невозможно без вас, вдумчивых и терпеливых читателей, интересующихся проблемами цифрового права, методологическими и содержательными изменениями в традиционных отраслях права, возникающих в эпоху цифровой экономики. Ваш интерес к нашему проекту способствует его постоянному развитию, улучшению качества публикаций и привлечению новых читателей, авторов и экспертов.

С огромной радостью мы рады представить вашему вниманию первый номер второго тома и надеемся, что 2021 год принесет успех нашему общему делу!

С наилучшими пожеланиями,

главный редактор,
кандидат юридических наук
М. И. Иноземцев

Список литературы / References:

1. Anagnostopoulou, D. (2018). The withdrawal of the common European sales law proposal and the European commission proposal on certain aspects concerning contracts for the online and other distance sales of goods. In M. Heidemann, & J. Lee (Eds.), *The future of the commercial contract in scholarship and law reform: European and comparative perspectives* (pp. 127–163). Springer, Cham. https://doi.org/10.1007/978-3-319-95969-6_6

2. Bachilo, I. L. (2001a). Aktual'nyye problemy informatsionnogo prava. [Actual problems of information law]. *Nauchno-Tekhnicheskaya Informatsiya*. *Seriya 1: Organizatsiya i Metodika Informatsionnoy Raboty*, (9), 3–8.
3. Bachilo, I. L. (2001b). *Informatsionnoye pravo* [Information law]. Yurinformtsentr.
4. Bachilo, I. L. (2001c). Informatsionnoye pravo. Rol' i mesto v sisteme prava Rossiyskoy Federatsii [Information law. Role and place in the legal system of the Russian Federation]. *Gosudarstvo i Pravo*, (2), 5–14.
5. Colomo, P. I. (2017). Copyright licensing and the EU digital single market strategy. In R. Blair, & D. Sokol (Eds.), *The Cambridge handbook of antitrust, intellectual property, and High Tech* (Cambridge law handbooks, pp. 339–357). Cambridge University Press. https://doi.org/10.1017/9781316671313.018
6. Danilenkov, A. V. (2014). *Internet-Pravo* [Internet law]. Yustitsinform.
7. Easterbrook, F. H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum*, *1996*, Article 7. https://chicagounbound.uchicago.edu/uclf/vol1996/iss1/7
8. Edwards, L., & Waelde, C. (Eds.). (2009). *Law and the Internet*. Bloomsbury Publishing.
9. Goldman, E. (2008). Teaching cyberlaw. *Saint Louis University Law Journal*, 52(3), 749–764.
10. Goloskokov, L. V. (2006). *Teoriya setevogo prava* (A. V. Malko, ed.) [Network law theory]. Izd-vo R. Aslanova.
11. Havu, K. (2017). The EU digital single market from a consumer standpoint: How do promises meet means? *Contemporary Readings in Law and Social Justice, 9*(2), 146–183. https://doi.org/10.22381/CRLSJ9220179
12. Kahin, B., & Nesson, C. (Eds.). (1997). *Borders in cyberspace: Information policy and the global information infrastructure*. MIT Press.
13. Kerr, O. S. (2003). The problem of perspective in Internet law. *Georgetown Law Journal*, *91*, 357–405.
14. Khabriyeva, T. Y., & Chernogor, N. N. (2018). Pravo v usloviyakh tsifrovoy real'nosti [Law in the context of digital reality]. *Zhurnal Rossiyskogo Prava*, *1*, 85–102. https://doi.org/10.12737/art_2018_1_7
15. KjØrven, M. E. (2020). Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe. *European Business Law Review*, *31*(1), 77–109. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020004
16. Kopylov, V. A. (1997). *Informatsionnoye pravo* [Information law]. Yurist.
17. Kopylov, V. A. (2001). Internet i pravo [Internet and law]. *Nauchno-Tekhnicheskaya Informatsiya. Seriya 1: Organizatsiya i Metodika Informatsionnoy Raboty*, (9), 8.
18. Langenbucher, K. (2020). Responsible A.I.-Based credit scoring — A legal framework. *European Business Law Review*, 31(4), 527–571. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.4/EULR2020022
19. Larouche, P. (2008). On the future of information law as a specific field of law (Discussion Paper No. 2008-020). Tilburg University: Tilburg Law and Economics Center.
20. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, *113*(2), 501–549. https://doi.org/10.2307/1342331
21. Manes, P. (2020). Legal challenges in the realm of InsurTech. *European Business Law Review*, *31*(1), 129–168. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020006
22. Marsden, C. T. (Ed.). (2000). *Regulating the global information society* (Vol. 2). Psychology Press.
23. Morozov, A. V. (1999). *Sistema pravovoy informatizatsii Minyusta Rossii* [The system of legal informatization of the Ministry of Justice of Russia]. Triumf.
24. Naumov, V. B. (2002). *Pravo i Internet: Ocherki teorii i praktiki* [Law and the Internet: Essays on theory and practice]. Knizhnyy Dom "Universitet".
25. Nikitin, E., & Marius, M. C. (2020). Unified digital law enforcement environment — Necessity and prospects for creation in the "BRICS countries". *BRICS Law Journal*, *7*(2), 66–93. https://doi.org/10.21684/2412-2343-2020-7-2-66-93

26. Rassolov, I. M. (2009). *Pravo i Internet. Teoreticheskiye problemy* (2nd ed.) [Law and the Internet. Theoretical Problems]. Norma.
27. Seidel, E., Horsch, A., & Eickstädt, A. (2020). Potentials and limitations of smart contracts: A primer from an economic point of view. *European Business Law Review*, *31*(1), 169–183. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.1/EULR2020007
28. Shagiyeva, R. V. (2005). *Kontseptsiya pravovoy deyatel'nosti v sovremennom obshchestve* [The concept of legal activity in modern society]. Izdatel'stvo Kazanskogo Universiteta.
29. Soldatov, A. S. (2002). *Pravo kak instrument sotsial'nogo upravleniya* [Law as an instrument of social management]. Yurist.
30. Sommer, J. H. (2000). Against cyberlaw. *Berkeley Technology Law Journal*, *15*(3), 1145–1232.
31. Zoboli, L. (2020). Fueling the European digital economy: A regulatory assessment of B2B data sharing. *European Business Law Review*, 31(4), 663–692. https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.4/EULR2020026

Сведения об авторе:

Иноземцев М. И. — кандидат юридических наук, доцент кафедры международного частного и гражданского права им. С. Н. Лебедева МГИМО МИД России, главный редактор журнала «Цифровое право» (Digital Law Journal), Москва, Россия.
inozemtsev@inno.mgimo.ru
ORCID 0000-0003-1845-1363

Information about the author:

Maxim I. Inozemtsev — Ph.D. in Law, Associate Professor, Department of Private International and Civil Law, MGIMO-University, Editor-in-Chief, Digital Law Journal, Moscow, Russia.
inozemtsev@inno.mgimo.ru
ORCID 0000-0003-1845-1363

https://doi.org/10.38044/2686-9136-2021-2-1-29-47

ARTICLES

DIGITAL TRANSFORMATION OF URBAN GOVERNANCE IN CHINA: THE EMERGENCE AND EVOLUTION OF SMART CITIES

Bo Qin[1,*], Su Qi[2]

[1]Public Policy Lab, Renmin University of China
59, Zhongguancun str., Haidian District, Beijing,
People's Republic of China, 100872

[2]Renmin University of China
59, Zhongguancun str., Haidian District, Beijing,
People's Republic of China, 100872

Abstract

This research article contributes to the field of digital governance as it reviews the conceptual definition and practical application of "smart cities" in the context of urban development in China. By analyzing both first-hand interview data and secondary statistical and policy reports during the period between 2009 to 2019, we contend that the emergence of smart cities in China has evolved from a disorderly process to a more standardized one. During this process, cities made efforts to use digital technology — such as 5G, cloud computing, and the Internet of Things — in social governance, infrastructure, and industrial development. However, such rapid development also spawned a series of emerging legal issues, which had a huge impact on China's legal system. The article seeks to holistically examine the discourse surrounding the concept of a "smart city" and its practical implementation by drawing attention to its promises as well as criticisms. The article also touches upon the challenges — such as "information islands" in construction, technology, and management — that confront the emerging smart cities, and emphasizes China's need to further improve laws and regulations, build an integrated legal system, explore new regulation methods, shape a highly autonomous and refined governance order, and provide legal protection for the development of smart cities. The paper concludes by mentioning possible areas for further research to find a developmental path for "smart cities" that can realize resource integration and sharing.

Keywords

smart city, urban governance, legal system, China

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study had no sponsorship.

For citation Qin, B., & Qi, S. (2021). Digital transformation of urban governance in China: The emergence and evolution of smart cities. *Digital Law Journal, 2*(1), 29–47. https://doi.org/10.38044/2686-9136-2021-2-1-29-47

* Corresponding author

Submitted: 19 Jan. 2021, accepted: 22 Feb. 2021, published: 31 Mar. 2021

СТАТЬИ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОРОДСКОГО УПРАВЛЕНИЯ В КИТАЕ: ГЕНЕЗИС УМНЫХ ГОРОДОВ

Б. Цинь[1,*], С. Ци[2]

[1]Лаборатория публичной политики, Университет Женьминь
100872, Китайская Народная Республика, Пекин, район Хайдянь, ул. Чжунгуаньцунь, 59

[2]Университет Женьминь
100872, Китайская Народная Республика, Пекин, район Хайдянь, ул. Чжунгуаньцунь, 59

Аннотация

Статья посвящена проблеме цифрового управления в умных городах на примере Китае. Проанализировав данные опросов и статистических и политических отчетов за период между 2009 и 2019 гг., авторы пришли к выводу, что хаотичный процесс появления умных городов в Китае приобрел более стандартизованный характер. В ходе цифровой трансформации городского управления использовались такие технологий как 5G, облачные вычисления и «интернет вещей» в социальном управлении, инфраструктуре и промышленном развитии. Тем не менее столь бурное развитие технологий породило ряд новых юридических проблем, оказавших значительное влияние на правовую систему Китая. Авторы предпринимают попытку системно осмыслить концепцию «умный город» и ее реализацию на практике путем привлечения внимания к перспективам и критике развития умных городов. Более того, в статье затрагиваются проблемы «информационных островов» в строительстве, технологиях и управлении, с которыми сталкиваются в процессе цифровой трансформации городского управления, а также подчеркивается необходимость дальнейшего совершенствования законодательства Китая, в создании интегрированной правовой системы и изучении новых методов регулирования. Особое внимание уделяется потребности сформировать автономный и усовершенствованный порядок управления и обеспечить правовую охрану развития умных городов.

Ключевые слова

умные города, городское управление, правовая система, Китай

Конфликт интересов Авторы сообщают об отсутствии конфликта интересов.

Финансирование Исследование не имело спонсорской поддержки.

Для цитирования Цинь, Б., Ци, С. (2021). Цифровая трансформация городского управления в Китае: возникновение умных городов. *Цифровое право, 2*(1), 29–47. https://doi.org/10.38044/2686-9136-2021-2-1-29-47

* Автор, ответственный за переписку

Поступила: 19.01.2021; принята в печать: 22.02.2021; опубликована: 31.03.2021

This research article reviews the conceptual evolution and practical application of the concept of a smart city in China. This concept has become popular in cities worldwide since its first proposal. It is regarded as a strategic choice to improve the efficiency of urban governance and the quality of public services, as well as to promote urban industrial transformation and urban sustainable development (Shengzu et al., 2013). In the past few decades, China has experienced rapid development in technology, such as the Internet of Things, big data, cloud computing, and artificial intelligence; this laid the foundation for smart cities. Many cities, such as Ningbo, Nanjing, Shenzhen, Shanghai, and Guangzhou, proposed the development of a "smart city" and issued various plans and policies to promote its implementation (Shengzu & Min, 2012). Recently, the technologies involved in developing a smart city have been widely used to support the prevention and control of the COVID-19 pandemic in China, including drug research and development, epidemiological investigation, epidemic visualization, analysis and prediction, auxiliary decision-making, intelligent architecture, online office and teaching, logistics and transportation, and so on. The benefits of smart cities have thus, to some extent, been tested in practice.

The Emergence and Evolution of Smart Cities

The Developmental Background of Smart Cities

In the 21st century, human society has significantly been transformed, with a "rural" world having turned into an "urban" one. According to the data released by the United Nations Department of Economic and Social Affairs, 55 % of the world's population lived in cities in 2018, while the number is expected to reach 68 % by 2050.[1] However, this rapid urbanization has also resulted in many problems pertaining to waste disposal, air pollution, resource shortages, health, traffic congestion, insufficient infrastructure, and many more. Worldwide, as cities are looking for smarter ways of dealing with such challenges, a "smart city" has been proposed as one way of dealing with such challenges (Alawadhi et al., 2012).

A notable feature of a smart city is the use of information and communication technology (ICT) infrastructure to improve economic efficiency and promote social, cultural, and urban development. It utilizes the new technological revolution represented by ICT, the Internet of Things, and cloud computing, which enabled cities to continuously improve their ability to perceive, process, integrate, and apply data, so that they can deal with more complex problems. In 2008, International Business Machines (IBM) put forward the vision of "smart earth", hoping to use advanced ICT to build a new world operating model

[1] Department of Economic and Social Affairs. (2019). *World urbanization prospects: The 2018 revision (ST/ESA/SER.A/420)*. United Nations. https://population.un.org/wup/Publications/Files/WUP2018-Report.pdf

and to explore new driving forces for urban development after the financial crisis. In 2009, IBM officially proposed the concept of "smart city" on the basis of the notion of "smart earth". It was proposed that a smart city should be able to make full use of ICT, responding intelligently to various needs of people's livelihood, environmental protection, public security, urban services, and industrial and commercial activities; this would create a better urban life for human beings.[2]

Notably, the concept of a smart city has been influenced by neoliberalism, which represents economic growth and business orientation (Hollands, 2008). In the face of increasing economic competition among cities, business-oriented development strategies have been accepted and implemented by many urban governments (Caragliu et al., 2011).

Conceptual Definition of a "Smart City"

Various definitions of a smart city have been proposed in different scholarly backgrounds (Table 1). As a smart city is based on ICT: some scholars and institutions put more emphasis on the role of technology, while others regard it from a broader perspective and eventually define it as an organic interconnected system.

A narrower perspective of a smart city emphasizes the application of technology to make urban infrastructure and services more intelligent, interconnected, and efficient (Washburn et al., 2010). This kind of intelligence and efficiency requires an instrumented urban environment. With the help of various sensors, electronic devices, and applications, the operational state of key urban infrastructure can be monitored and integrated (Harrison et al., 2010) to form a self-monitoring and self-reaction mechanism of the city itself.[3] Processing various data with the help of technology can optimize the function of urban infrastructure, provide more efficient services, and promote economic cooperation and innovation (Marsal-Llacuna et al., 2015). This definition of a smart city has technology at its core and is committed to creating a smart urban environment to improve the efficiency of urban operation and realize economic growth. However, less attention is paid to urban economic, cultural, and social activities as conducted by human beings, and thus it has been criticized for being too technology-oriented (Hollands, 2008).

The narrower definition of a smart city gives a technical pathway, while the broader definition provides a comprehensive vision of urban governance involving more fields. Giffinger[4] offers a comprehensive definition of a smart city that includes six aspects: smart economy, smart governance, smart environment, smart people, smart mobility, and smart living. This is a more operational definition that is important in guiding the practice of a smart city. Neirotti (2014) give an even broader definition and divided smart cities into six dimensions which include natural resources and energy, transport and mobility, buildings, living, government, economy, and people.

A smart city, in a broad sense, involves many different dimensions. Nam and Pardo (2011) structured it into three dimensions: technology, people, and system, which not only includes the narrower sense of technology, but also summarizes the content of people and institution in the broad concept. A more simplified and abstract definition summarizes these dimensions into "hard field" and "soft field". The former includes energy, transport, environment, and buildings, while the latter includes

2 IBM. (n.d.). IBM *Research — China*. Retrieved January 7, 2020. https://www.research.ibm.com/labs/china/index.shtml

3 Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Wimmersperg, U. (2000, September 28). The vision of a smart city. Paper presented at the Proceedings of the 2nd International Life Extension Technology Workshop, Paris, France.

4 Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. (2007). Smart cities: Ranking of European medium-sized cities (Report). Vienna University of Technology. https://gretere.miigaik.ru/sites/default/files/materials/3_00_Ranking%20of%20European%20medium-sized%20cities.pdf

Table 1

Definitions of a Smart City

Definition	Source
The use of Smart Computing technologies to make the critical infrastructure components and services of a city (which include city administration, education, healthcare, public safety, real estate, transportation, and utilities) more intelligent, interconnected, and efficient.	(Washburn et al., 2010)
A city connecting the physical infrastructure, ICT infrastructure, social infrastructure, and business infrastructure to leverage the collective intelligence of the city.	(Harrison et al., 2010)
A city that monitors and integrates the conditions of all its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, and even major buildings, so it can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens.	(Hall, 2000)
Smart city initiatives try to improve urban performance by using data, information, and ICT to provide more efficient services to citizens, to monitor and optimize existing infrastructure, to increase collaboration among different economic actors, and to encourage innovative business models in both the private and public sectors.	(Marsal-Llacuna et al., 2015)
A city performing well in a forward-looking way in the economy, people, governance, mobility, environment, and living, built on the smart combination of endowments and activities of self-decisive, independent, and aware citizens. A smart city generally refers to the search and identification of intelligent solutions which allow modern cities to enhance the quality of the services provided to citizens.	(Giffinger et al., 2007)[5]
A city is smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance.	(Caragliu et al., 2011)
Smart cities as territories with a high capacity for learning and innovation, which are built in the creativity of their population, their institutions of knowledge creation, and their digital infrastructure for communication and knowledge management.	(Komninos, 2011)
A smart city infuses information into its physical infrastructure to improve convenience, facilitate mobility, add efficiencies, conserve energy, improve the quality of air and water, identify problems and fix them quickly, recover rapidly from disasters, collect data to make better decisions, deploy resources effectively, and share data to enable collaboration across entities and domains.	(Nam & Pardo, 2011)

[5] Giffinger et al., 2007.

Continuation of Table 1

Definition	Source
A smart city can make full use of information and communication technologies to sense, analyze, and integrate the information of the core system of city operation to make smart responses to various demands, including people's livelihoods, environmental protection, public safety, urban services, industrial and commercial activities, and to create a better urban life for mankind.	(Smart city in China, 2009)[6]
A smart city is based on the basic framework of a "digital city". It is connected with "real city" through ubiquitous sensor network, and automatically controls various facilities by a cloud computing platform, which can store, compute, and analyze massive data and assist in decision making.	(Deren et al., 2014)
The smart city is a reform and innovation system project carried out under the conditions of the modern information society, aiming at the practical needs of urban economic and social development, with the core aim of improving people's happiness and satisfaction to promote the wisdom of the urban development mode.	(Sisi et al., 2020)

education, culture, social welfare, public management, and economy (Neirotti et al., 2014). However, the simple combination of these dimensions cannot create a smart city. Instead, it should be regarded as an organic network or system, in which the relationships among urban sub-systems need to be considered.[7]

In summation, the definition of a smart city can be divided into three categories. The first type pays attention to the extensive and in-depth application of new generation ICT in cities. It points out that a smart city is one that integrates and improves urban operation systems through ICT. The second one attaches importance to the comprehensive development of the economy, society, culture, and environment based on ICT. The third one emphasizes the dynamic process of a smart city's development and regards it as an organic innovation process carried out by cities using ICT[8] These definitions seem to have a progressive evolutionary process. Information and communication technology is the important foundation for cities to realize "smart" development, while human wisdom is the soul of smart cities. The goal of smart cities is to realize the comprehensive sustainable development of the economy, society, and environment, which requires breaking through and transcending the traditional urban governance mode.

Components of a Smart City

The components of a smart city are in line with above-mentioned definitions. Scholars who define smart cities from a narrow perspective usually focus on the technical level and divide the idea of

[6] China Information and Communication Research Institute (CICRI). (2019, November 13). Xīn zhìhuì chéngshì de fāzhǎn [Development of new smart cities]. https://mp.weixin.qq.com/s/hJ3ZMn70gU11wuk5EjPavQ

[7] Kanter, R. M., & Litow, S. S. (2009). Informed and interconnected: A manifesto for smarter cities. (Working Paper No. 09-141). Harvard Business School. https://www.hbs.edu/faculty/Pages/item.aspx?num=36185

[8] Xiaojuan, Z. (2015). *Zhìhuì chéngshì xìtǒng de yāo sù, jiégòu jí móxíng yánjiū* [The elements, structure and model of smart city system] [Unpublished doctoral dissertation]. South China University of Technology.

a smart city into its perception layer, network layer, and application layer. The so-called perception layer refers to the acquisition of basic data of the city based on the equipment for perceiving, measuring, capturing, and transferring information, such as radio frequency identification, infrared sensors, global positioning systems, laser scanners, mobile phones, etc. The network layer uses the internet, the Internet of Things, and information platforms to process, integrate, interact, and share scattered information, and explore the practical significance of city data by identifying problems of the city. The application layer is the most intuitive embodiment of a smart city's promotion of urban development. It provides corresponding data supports or decision-making services for the various functions and needs of the city. It is also a more differentiated level, including smart logistics, smart energy, smart transportation, smart tourism, smart medical care, smart environmental protection, etc. (Deren et al., 2014).

The conceptual framework of a smart city, in a broader sense, truly treats it as a city operation model. It does not only treat smart infrastructure, smart governance, and smart public services as derivative applications of technologies, but also considers them as basic parts of urban operation and integrates them into a more ambitious urban operation structure. Therefore, this elemental framework can be understood as the top-level design of a smart city and is the overall strategy guiding its development (Xibo & Zaigao, 2010).

The Practical Applications of Smart Cities in China

The Development History of Smart Cities

Smart cities in China have developed over a decade, during which the government and enterprises have explored different ways to cooperate (Table 2). The whole process can be divided into three phases (Table 3).

The first phase took place from 2008 to 2012, which was the period in which the concept of a smart city was introduced. After the publication of "Smart Cities in China" by IBM in 2009, IBM began to cooperate with Chinese city governments, enterprises, and scholars to promote the construction of smart cities. Therefore, the early practice of smart cities in China was a commercial activity rather than a government initiative (Wang et al., 2013).

The second phase unfolded from 2012 to 2015, which was the pilot period of exploring the concept of a smart city. This was a period of promoting the smart city pilot projects, with pilot projects also being a common method in China for implementing policies. Due to a lack of coordination among various departments, there had been many different pilots in the smart city's construction, leading to a certain degree of confusion in the initial stage. Among these different pilots, those by the Ministry of Housing and Urban-Rural Development had the largest influential power; it has promoted 290 pilot cities in three batches. Since 2014, the construction of smart cities began to be standardized at the national level. The "Inter-Ministry Coordination Working Group for Promoting the Healthy Development of Smart City" was established, and the "Guiding Opinions on Promoting the Healthy Development of Smart Cities" were formulated to coordinate the work of various departments. At the same time, driven by emerging technologies such as 3G, 4G, and cloud computing, pilot cities began to explore local cooperation in various business application fields. The construction of smart cities has gradually been brought on the right track (Sisi et al., 2020).

Table 2

Smart City Pilot Projects in China

Time	Department	Name of the pilot	Number
2010	Ministry of Science and Technology	Pilot cities of National 863 Smart City Project	2
2012	Chinese Academy of Engineering	"China Smart City" pilot city	5
2014	Ministry of Industry and Information Technology	Pilot and demonstration cities for building a smart city	2
2013	National Administration of Surveying, Mapping and Geographic Information	Pilot cities of smart city space-time information cloud Platform	10
2013	Ministry of Housing and Urban-Rural Development	The first batch of national smart city pilot cities	90
2013	Ministry of Industry and Information Technolog, Ministry of Environmental Protection, etc.	Smart City Demonstration Pilot Project	6
2013	Ministry of Housing and Urban-Rural Development	The second batch of national smart city pilot cities	103
2013	Ministry of Industry and Information Technology	Pilot demonstration area of application of public platform of e-government based on cloud computing	59
2013	Ministry of Science and Technology, National Standards Commission	The National Smart City Pilot and Demonstration City	20
2013	National Development and Reform Commission, Ministry of Industry and Information Technology	Pilot cities for China-EU Smart City Cooperation	15
2013	Ministry of Industry and Information Technology	National information consumption pilot cities	68
2014	National Development and Reform Commission	Information benefit people national pilot city	80
2015	Ministry of Housing and Urban-Rural Development, Ministry of Science and Technology	The third batch of national smart city pilot cities	97

Table 3

Development History of Smart Cities in China

	Concept import (2008–2012)	Pilot exploration (2012–2015)	Coordinated advancement (2016–2020)
Driving mode	Industry application driven	Emerging technology driven	Data driven
Key technology	Wireless communication, fiber optic broadband, information distribution technology such as HTTP, GIS, GPS, RS	RFID, 2G/3G/4G, Cloud Computing, S OA	5G, Big data, artificial intelligence, blockchain, Smart City platform and OS
Information sharing	Single system, scattered construction, spontaneous sharing	Horizontal and vertical division, share with key projects or applications	Horizontal and vertical system integration, sharing according to functions
Development characteristics	Enterprise introducing concept, Foreign software system integrators, IBM, Oracle	The ministries and commissions of the State take the lead in carrying out pilot construction, equipment manufacturers, integrators horse racing enclosure	National coordination, linkage of 25 ministries and commissions, government guidance, market leadership, Public-Private Partnership, domestic internet enterprises, operators, software providers and integrators all gather together

The third phase was launched in 2016. The development concept, construction idea, implementation path, operation mode, and technical means of a smart city have all been upgraded.[9] The concept of a smart city has been regarded as a national strategy for new urbanization and industrial transformation. A series of supporting policies and plans have been introduced which has formed the government-guided and market-led pattern. Some new commercial activities and smart services are emerging, making up a ubiquitous idea of smart living.

Contents of Smart City Practices

Until now, the content of China's smart city policy has been comprehensive. In addition to infrastructure, application platforms, smart economy, smart governance, and smart ecology, policy and standards, top-level design, and related security measures are also involved.

Policy and Standards

Since the promulgation of the "Interim Management Measures for National Smart City Pilots" in 2012, China has issued a series of policies, technology standards, and evaluation standards for smart cities at the national and provincial levels (Table 4). These policies and standards can provide guidance for the development of smart cities at various stages.

[9] CICRI, 2019.

Table 4

Relevant Policy and Standards for Smart City in China

Release time	Name of policy or standard	Related content
2012	Interim Administrative Measures for National Smart City Pilot Project	Guiding the application, implementation, and management of national smart city pilot projects
2012	National Smart City (District, Town) Pilot Indicator System (Trial)	Making clear the indicator system of the smart city pilot
2013	Several Opinions on Promoting Information Consumption and Expanding Domestic Demand	Accelerating the development of smart cities
2014	Notice on Accelerating the Implementation of the Information Project for the Benefit of the People	Promoting the work of smart cities from the perspective of improving the quality of life with ICT
2014	National New Urbanization Plan (2014–2020)	Putting forward the key points and requirements promoting the construction of a smart city
2014	Guidelines on Promoting the Healthy Development of Smart Cities	Putting forward the development idea, construction principle, main goal, and information security guarantee of China's smart city
2015	Guidance on the Construction, Application, and Implementation of Smart City Standard System and Evaluation Index System	Accelerating the formulation of relevant standards, and putting the standardization of smart cities on the national agenda
2016	Task Division of Inter-Ministerial Coordination Working Group on New Smart City Construction (2016–2018)	Clarifying the tasks and responsibilities of the 25 member departments of the Inter-ministerial Coordination Working Group
2016	Evaluation Index of New Smart City (2016)	Making clear the evaluation index of a smart city
2017	Technical Outline for the Construction of Smart City Space-time Big Data Platform (2017 Edition)	Realizing the promotion of smart city's space-time benchmark, space-time big data, and space-time information cloud platform
2018	Evaluation Index of New Smart Cities (2018)	Updating the evaluation index of smart cities
2019	Technical Outline for the Construction of Smart City Space-time Big Data Platform (2019 Edition)	Further developing the space and time big data platform for smart cities

Top-Level Design

The continuous expansion of smart cities has resulted in a constant increase in the complexity of this systematic project. Strengthening the top-level design of smart cities is the primary step to make this work efficiently and orderly. In January 2019, China formally implemented the "Guidelines for Top-Level Design of Smart Cities", so that top-level design and overall planning have become a prerequisite for the implementation of smart cities. The proportions of national-level urban agglomerations, national-level new districts, provincial capital cities and cities separately listed in the state plan, prefecture-level cities, and county-level cities in developing smart cities' top-level designs or overall plans are 23 %, 52 %, 94 %, 71 %, and 25 % respectively.[10]

Infrastructure

Chinese cities have different key points when promoting smart cities, but ICT is always the foundation of such cities. Earlier infrastructure construction, which was based on broadband, 3G, and 4G, has shifted to new infrastructure, instead incorporating 5G, the Internet of Things, and cloud computing. Beijing, Shanghai, Guangzhou, Shenzhen, Chongqing, Chengdu, Hangzhou, and Shenzhen have almost achieved 5G coverage as of now. Regarding the Internet of Things, five new industrial demonstration bases have been established at the national level, such as Wuxi and Hangzhou.

Application Platform

With the continuous accumulation of urban data, as well as the in-depth application of various technologies such as big data, artificial intelligence, and blockchain, the integration of key common capabilities will be strengthened to eliminate the problem of data islands. The urban big data platform, which originated from the early days of the sharing exchange platform regarding government affairs, has gradually expanded to other fields. It has incorporated various data such as urban operation perception data, enterprise data, and internet data, which has made it the core component platform of a smart city. With the mature application of new surveying and mapping, analog simulation, deep learning, and other technologies, the construction of one-to-one mapping digital twin cities in the digital space is becoming a new exploration in Xiong'an and Chongqing.

Smart Living

The construction of a "smart city" has fully entered a new stage with service at the core. Smart government services have been popularized, and services that benefit the people and enterprises within reach have in recent years become the development focus of a smart city. With the in-depth advancement of "internet + government service", the convenience of online administration of government services has been continuously improved. Online inquiries and the online handling of public services have basically been popularized nationwide. Some areas have adopted government big data, government service robots, and other intelligent means to promote government affairs, data standardization, service networking, and processing automation. For example, "appropriation with the application" in Shanghai and "Guangdong Provincial Affairs" in Guangdong Province can help citizens to obtain one-stop services such as government services, payment, e-commerce, travel, and meal ordering, realizing multiple channels and a wide coverage of services. These kinds of apps are becoming the new infrastructure pertaining to public services.

[10] CICRI, 2019.

Smart Economy

At present, 23 provincial-level regions in China have introduced top-level designs in the digital economy. With the core concept of "industry-city integration", the construction of smart cities will help in promoting two-way data circulation between governments and enterprises, cultivating several leading digital service companies, and exploring a win-win pattern for urban transformation and industrial innovation. Overall, China's digital industry is still led by the four major clusters of the Beijing-Tianjin-Hebei, Yangtze River Delta, Pearl River Delta, and Chengdu-Chongqing urban agglomerations.

Smart Governance

The development and innovative applications of the new generation of ICT have greatly improved social governance capabilities and promoted smart city governance methods that are more digital, networked, and intelligent. "Internet + supervision" has gradually developed into an effective means of strengthening in-process and post-event supervision. Many cities make full use of big data and social credit systems to strengthen the tracking and early warning of market risks. For example, Beijing relies on the Enterprise Credit Information Network to list 200 000 enterprises in the list of business abnormalities, and uses big data technology to effectively control market supervision risks and to implement cross-department joint credit punishments on untrustworthy enterprises. In the field of urban security, Baidu is building an intelligent video surveillance platform for a smart city and smart security, providing full-process services including camera equipment management, video stream access, video frame extraction, video analysis, and alarm information display. The platform has the ability of surveilling helmet wearing compliance testing, work clothes compliance testing, fireworks testing, stranger recognition, smoking recognition, and mobile phone recognition.

Smart Ecology

The concept of green sustainable development is an important component of smart cities. Driven by technological innovation and the demand for sustainable development, many cities are actively exploring greener and lower-carbon production and lifestyles and promoting more precise ecological monitoring. The 5G integrated ecological detection system built by Xiong'an New Area utilizes the high speed and low latency of 5G, as well as the all-weather and all-terrain inspection features of drones and unmanned ships, to realize the ecological conditions and water quality monitoring of Baiyangdian. Its data are instantly uploaded to the platform for analysis, and it supports the staff to observe the analysis results and on-site conditions through monitoring screens and virtual reality (VR) glasses.

Data Security

While the development of smart cities brings more convenient services to the public, the increased complexity of network platforms also simultaneously brings about the problem of digital space security. "Personal privacy protection" and "autonomy and trustworthiness" have become the focus of attention. The national level continues to increase the high-pressure supervision of data collection in violation of mobile application services. The Central Cyberspace Affairs Office is cooperating with the other four ministries to set up the "Special Task Force on App collection and use of personal information in violation of laws and regulations". The Special Task Force aims to evaluate mobile applications in key areas, sort out the "blacklist" of illegal applications, and carry out supervision and rectification work.

Operation Models of a Smart City

Smart cities involve not only the evolution of the established concepts and the construction of infrastructure, but also the models of investment, operation management, and profit need, in order to enable the sustainable development of smart cities and to allow more people to benefit from them. In the process of developing a smart city, local governments have explored and developed some models to clarify the roles of government and enterprises.

Institutional Setting

The construction of smart cities is a systematic project involving a wide range of areas. Overall, specialized smart city management agencies in China are divided into two categories. The first one is the newly established Big Data Bureau, or other such specialized agencies which manage the construction of a smart city. At present, many cities have set up big data authorities with data resource management as the core function and are becoming the main institutions for data integration and sharing. According to our survey data, 277 cities across the country have established Big Data Bureaus or similar specialized agencies. The second one is the responsibility assumed by the Ministry of Industry and Informatization, the Development and Reform Commission, and the Cyberspace Administration of China. Tianjin, Hebei, Liaoning, Shanghai, Jiangsu, Zhejiang, and some other provinces have assumed responsibility.

Investment Models

Developing smart cities requires high levels of infrastructure and technological innovation, and a large amount of capital investment. From the perspective of operating funds, Wang et al. (2013) summarized the investment of smart cities into three models. First, the government independently invests in network construction and is responsible for maintenance. This model is mostly used in government affairs and some public service fields in which the main purpose is not to make profit. Second, the government takes the lead and is responsible for major investments, while the commissions operators provide relevant support and obtain some particular benefits or subsidies. This type of model gives the government higher regulatory capabilities, but the operators have little influence on product planning and layout. Third, the government provides limited infrastructure and policy support, and operators are responsible for the main investment, construction, and operation (Wang et al., 2013). In the initial stage of the construction of smart cities in China, local telecom operators were the mainstay, and then the local government was gradually encouraged to cooperate with social capital. Some technology companies and social capital, such as Alibaba and Huawei, began participating. The construction of smart cities has evolved from a single government-led model to a diversified model of social participation and joint construction and operation.

Operation Models

At present, among the 657 cities that carried out data monitoring, 433 (accounting for 65.91 %) have developed smart city projects with non-governmental agencies (firms and NGOs) acting as the main body. With the upgrading of a smart city, new operating models and the relationship between government and enterprises have emerged, giving rise to the role of “smart city operators” to coordinate the construction, operation, and management of smart cities.

Smart city operators can be divided into two categories. The first is where the government and enterprises cooperate to establish specialized operating companies. This model could be described as “government-enterprise cooperation, the separation of management and operation”, which is the

innovation of Guangdong's "digital government" reform. The government departments took greater management responsibilities for analyzing needs and evaluating services. Tencent, China Mobile, China Unicom, and China Telecom jointly funded the Digital Guangdong Network Construction Co. Ltd., which assumed the operating responsibilities, including a series of tasks such as standard formulation, demand docking, data fusion, and system operation. The other category is to carry out the smart city initiatives that rely on large companies. In Zhejiang, Alibaba has proposed its being an in-depth partner not only for business cooperation but also for all aspects of planning, design, construction, and services.

Profit Models

The construction and maintenance of smart cities require a large amount of capital investment, which is financially difficult for the government to bear. Therefore, the development of smart cities must form a clear profit model to ensure sustainability.

At present, the profit model of smart city projects is mainly divided into three categories. The first is to accumulate users and monetize network flow. This entails accumulating many users through smart tourism, smart education, and other projects, and then providing value-added services to monetize network flow. For example, Tencent cooperated with the Puzhehei government in Yunnan Province to build a smart scenic spot, relying on a large amount of tourist information to develop "tourism installment", "tourism loan", and other business schemes.

The second is based on contract management and revenue sharing. For example, for a smart streetlight project invested by a company, the government will repay the saved electricity bills to the company in installments. When the contract management expires, the smart streetlight will be transferred to the government free of charge. This zero-government investment model effectively solves the problem of lack of funds and realizes the "three-win" situation of government saving money, social energy saving, and corporate profits.

The third is data desensitization and limited operation. The desensitized data is leased to an enterprise for further exploration of their potential commercial value. For example, in an Urban Smart Campus Project, the campus monitoring, campus surrounding monitoring, and school bus monitoring are integrated and opened to professional operating companies through the integrated urban operation platform. The operating companies can provide paid services to the government, schools, and parents, whilst allows parents to track their children's activity through the application.

The Challenge Facing the Adoption of a "Smart City" Model

Smart cities are the product of technology and an urban development; in a short period, this has hugely influenced and nurtured many emerging businesses in China. Such rapid development will inevitably impact the original social legal order and pose unforeseen danger for the development of cities. Poor laws and regulations, similar / uniform / monotonous conceptions of smart cities, and isolated information islands are some of the challenges that should be resolved in future.

Legal Challenges

The development of smart cities depends on the advancement of related technologies such as the Internet of Things, big data, and artificial intelligence. This has created a double-layered space between the networked society and the real society, which is characterized by the coexistence of

humans and machines (Changshan, 2018). This new social organization has profoundly changed legal values, legal relations, and legal practices.

In terms of legal practice, the current smart city construction mainly involves two legal issues: one for "people", the other for "things". Specifically, it includes the issue of the civil subject of the legal qualification of robots (Yujie, 2017), the copyright issue of works generated by artificial intelligence (Zhiwen, 2017), the tort law issue of human damage caused by intelligent systems (Handong, 2017), the personal rights issue of human data privacy protection (Wei, 2016), the traffic law issues of intelligent driving systems (Xiao & Jianfeng, 2017), the labor law issues of machine "workers" (Handong, 2017), and so on. These emerging issues have posed a huge challenge for China's existing legal system.

Firstly, existing legal norms are difficult to adjust and ineffectively cover legal interests. The development of smart interconnection has spawned many emerging things and businesses, such as smart contracts, virtual currencies, online shopping, ride-hailing, etc. These have formed an unprecedented relationship and fashioned a new framework of rights and obligations; for existing legal concepts, rules, and principles, this is difficult to effectively cover. Secondly, it is becoming increasingly difficult for this to be explained effectively by China's existing civil and commercial laws, theories, and rules. In the context of a smart city, data resources have become important factors of production and social wealth. A series of platform companies, such as Tencent, Taobao, and JD, are constantly excavating and analyzing data to realize their own business interests. However, the nature, classification, ownership, usage rules, and legal responsibilities of data and information lacks explanatory power in this regard.

In addition, various platforms, based on their business type and operational needs, have the right to self-regulate the marketing order of the platform themselves. The government has no time or ability to supervise the huge, ever-changing, and technical platform transactions. Instead, review management power has been granted to platforms in the form of laws, regulations, or rules. They have the rights to formulate platform rules, penalize platform violations, and resolve platform disputes, which are the powers of quasi-legislation, quasi-enforcement, and quasi-judicial. This undoubtedly affects government intervention and market self-discipline, and the concepts, principles, and regulatory methods of administrative law have also encountered challenges (Changshan, 2018).

Finally, the existing judicial dispute resolution mechanism has also encountered obvious obstacles. The intelligent, hierarchical, and fragmented characteristics of internet crime make it difficult to adapt to the crime detection system based on traditional geographical and hierarchical jurisdiction. The detection rate of crimes such as cyber fraud is low, but the cost is high. Although China has established an internet court in Hangzhou, it lacks a clear legal system and clear responsibilities. There are still many issues that need to be resolved for the court in terms of jurisdiction, trial procedures, case trials, and judgment enforcement.

Taking the China National Health Code as an example, the promotion of the health code has become a pioneering work in China's epidemic prevention and control; however, it also runs personal information security risks. On the one hand, a large amount of sensitive personal information is concentrated under government control with the risk of personal information leakage; on the other hand, the handling of personal information lacks legal guidelines, and there are a large number of personal information processing activities that ignore the principle of informed consent and exceed the principle of minimum use and disclosure (Yuan, 2020).

In the field of data security, Europe and the United States have already conducted some legal explorations. The United States has passed the Consumer Privacy Bill of Rights Act of 2015 (CPBR), introduced a new scenario-led personal information protection mechanism, and taken the lead in

breaking through the current global structural model. The EU has added new mechanisms such as data breach notification, privacy impact assessment, and third-party certification in its draft "General Data Protection Regulation" (GDPR), highlighting new concepts such as scenario orientation and risk assessment (Wei, 2016).

China implemented the Cyber Security Law in 2017, but it is not maneuverable enough, with less than a half of normative clauses (Qin, 2020). China still lacks clear legislation aiming at data privacy and security, and relevant regulations mainly rely on regulatory documents of government departments. At the national level, China has enacted "Guiding Opinions on Promoting the Healthy Development of Smart City". At the same time, Shenzhen, Shanghai, Yinchuan, Tianjin, and other cities have also issued relevant documents on information security, which put forward requirements for data security management; nevertheless, their legal validity and enforcement binding have some limitations. At present, the relevant laws, regulations, systems, and policies in the field of smart cities need further improvements to promote their safe, healthy, and orderly development.

Commercial Challenges

Although the concept of a smart city has become the development model chosen by many, it is prudent to highlight some of the criticisms raised against this concept. The definition of a smart city has always been relatively vague, often associated with an intelligent, creative, and digital city. It regularly implies a relationship between technological progress and political, economic, and cultural changes. The hype of these terms is difficult to separate from the real practice, and eventually they are used more for the purpose of city marketing wherein some emerging cities are advertised as "smart cities" (Hollands, 2008).

These cities pay more attention to business-led urban development, hoping to use network infrastructure to improve economic and political efficiency and promote social, cultural, and urban development. However, their focus is on specific high-tech and creative industries. Hollands believes that a smart city has a technological determinism and capital dependence tendency to some degree but pays insufficient attention to people; at the same time, he also questioned the environmental sustainability of a smart city (2008). An important question is whether a smart city is truly environmentally friendly; the ICT revolution may not be as environmentally friendly as it initially seemed (Hollands, 2008). Even in some cities that truly practice the principles of a "smart city", they have introduced specific technical parameters to distinguish between "good" and "bad" cities, leaving a new moral order for cities. Therefore, the discourse of a smart city may be a powerful tool for generating docile subjects and political legitimization mechanisms (Vanolo, 2013).

The construction of smart cities in China initially had obvious commercial tendencies. After a period of governmental guidance, companies still play a pivotal role. This confirms Hollands' criticism of a smart city's commercial orientation. The result is that many cities rushed into mass action. China carried out "smart city" construction in more than 320 cities in 2012. The local governments followed the experience of urban construction and formed path dependence, which restricts the innovation and development of cities. The practices and functions of every smart city are very similar, so effective complementary relationships cannot be formed between cities (Shengzu et al., 2013). Due to the lack of a reasonable top-level design, blindly following the trend has also led to the inadequate understanding of a "smart city" in some cities. They either only emphasize the informatization projects, or include all kinds of irrelevant tasks into the scope of a smart city (Biyu et al., 2015). Besides, the technological orientation and capital-dependency of smart cities have formed a spatial aggregation

and imbalance. There is a clear gap in the construction level between the east and the west, and between cities of different levels (Liying & Chao, 2019).

Information Fragmentation Challenges

As IBM said, a smart city can make full use of ICT to sense, analyze, and integrate various information in the core system of city operation.[11] After more than ten years of development, China's current smart city projects still face information islands as the biggest obstacle to resource integration.

At the technical level, the notion of a smart city covers many areas but currently lacks uniform guiding standards in terms of construction, operation, and evaluation. The interfaces between different systems are complicated, which makes it difficult to achieve system interconnection, information sharing, and coordination. At the practical level, although various departments in the city have accumulated massive amounts of data and information in the long-term informatization application, the independence and segmentation of each system and the lack of scientific and effective information sharing mechanisms have led to many informatization islands. At the management level, it is difficult for urban departments to coordinate horizontally; administrative and managerial divisions are widespread. Some collaborative problems are often technically easy to solve but practically difficult to address within the management systems (Shengzu et al., 2013).

Conclusion

As a solution to urban problems, particularly after the 2008 economic crisis, the notion of a smart city has opened new development paths for cities. Relying on the sudden emergence of 5G, cloud computing, the Internet of Things, and other technical fields, China has made relatively outstanding progress in the construction of smart cities. China has built up mature basic technical facilities and application platforms, and related technologies are widely used in the fields of economy, governance, and general life. At the same time, results evaluation and sustainable models are also constantly being explored. These achievements have brought groundbreaking changes to China's urban development in the past decade. However, apart from such achievements, there are still barriers such as "information islands" in construction, technology, and management. These tremendous changes have also led to the criticisms of "labeling" and "urban marketing" being levelled at a part of so-called smart cities, which has brought new challenges to China's economic, legal, and social orders.

In the future, China needs to further improve laws and regulations, build an integrated legal system, explore new regulation methods, shape a highly autonomous and refined governance order, promote effective law enforcement, justice, embed risk control institutional mechanisms, maintain a good legal order, and provide legal protection for the development of smart cities. At the same time, the supervision of smart cities should be strengthened through reasonable evaluation to weaken the marketing motivation of some cities using the "smart city" model as a gimmick. In addition, further research in the fields of technology and management is needed to eliminate "information islands" and find a "smart city" development path that can realize resource integration and sharing.

[11] CICRI, 2019.

References:

1. Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., Nam T., Pardo, T. A., Scholl H. J., & Walker, S. (2012). Building understanding of smart city initiatives. In Scholl H.J., Janssen M., Wimmer M.A., Moe C.E., & Flak L.S. (Eds.), *Lecture notes in computer science: Vol. 7443 LNCS. Electronic government* (pp. 40–53). Springer. https://doi.org/10.1007/978-3-642-33489-4_4
2. Biyu, W., Junlan, L., Weiru, Z., Dong, J., & Guoqiang, Z. (2015). Analysis on practice of smart city pilot. *Modern Urban Research, 1*, 2–6. https://doi.org/10.3969/j.issn.1009-6000.2015.01.001
3. Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. *Journal of Urban Technology, 18*(2), 65–82. https://doi.org/10.1080/10630732.2011.601117
4. Changshan, M. (2018). Legal changes in the era of the intelligent Internet. *Chinese Journal of Law, 40*(4), 20–38. http://www.faxueyanjiu.com/Magazine/Show?ID=69344
5. Deren, L., Yuan, Y., & Zhenfeng, S. (2014). Big data in smart city. *Geomatics and Information Science of Wuhan University, 39*(6), 631–640. https://www.cnki.net/kcms/doi/10.13203/j.whugis20140135.html
6. Wang, G. B., Lei, Z., & Honglei, L. (2013). Guo nei wai zhi hui cheng shi li lun yan jiu yu shi jian si kao [Theoretical research and practical consideration of smart city in China and abroad]. *Science & Technology Progress and Policy, 30*(19), 153–160. http://caod.oriprobe.com/articles/40698520/guo_nei_wai_zhi_hui_cheng_shi_li_lun_yan_jiu_yu_shi_jian_si_kao_.htm
7. Handong, W. (2017). Réngōng zhìnéng shídài de zhìdù ānpái yǔ fǎlǜ guīzhì [Institutional arrangement and legal regulation in the era of artificial intelligence]. *Oriental Law, 5*, 98. http://www.iolaw.org.cn/showNews.aspx?id=61404
8. Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for smarter cities. *IBM Journal of Research and Development, 54*(4), 1–16. https://doi.org/10.1147/JRD.2010.2048257
9. Hollands, R. G. (2008). Will the real smart city please stand up? *City, 12*(3), 303–320. https://doi.org/10.1080/13604810802479126
10. Komninos, N. (2011). Intelligent cities: Variable geometries of spatial intelligence. *Intelligent Buildings International, 3*(3), 172–188. https://doi.org/10.1080/17508975.2011.579339
11. Liying, Y., & Chao, Z. (2019). Zhōngguó zhìhuì chéngshì lǐlùn yánjiū zòngshù yǔ shíjiàn jìnzhǎn [A review of the theoretical research and practical progress of smart city in China]. *E-Government,* 1, 111–121. http://www.cnki.com.cn/Article/CJFDTotal-DZZW201901018.htm
12. Washburn, D., Sindhu, U., Balaouras, S., Dines, R. A., Hayes, N. M., & Nelson, L. E. (2010). *Helping CIOs understanding smart city initiatives: Defining the smart city, its drivers, and the role of the CIO*. Cambridge.
13. Marsal-Llacuna, M.-L., Colomer-Llinàs, J., & Meléndez-Frigola, J. (2015). Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities Initiative. *Technological Forecasting and Social Change, 90*(B), 611–622. https://doi.org/10.1016/j.techfore.2014.01.012
14. Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th Annual International Conference on Digital Government Research Conference: Digital Government Innovation in Challenging Times*, 282–291. https://doi.org/10.1145/2037556.2037602
15. Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in smart city initiatives: Some stylized facts. *Cities, 38*, 25–36. https://doi.org/10.1016/j.cities.2013.12.010
16. Qin, Z. (2020). Zhìhuì chéngshì zhìlǐ zhōng gèrén xìnxī de quányì jiěxī hé quánlì bǎohù [Rights and interests analysis and protection of personal information in the management of smart cities]. *Social Sciences in Nanjing, 11*, 93–97. https://kns.cnki.net/kcms/detail/detail.aspx?doi=10.15937/j.cnki.issn1001-8263.2020.11.013

17. Shengzu, G., Jianwu, Y., & Jiangri, L. (2013). Dāngqián wǒguó zhìhuì chéngshì jiànshè zhōng de wèntí yǔ duìcè [Problems in the development of smart city in China and their solution]. *China Soft Science Journal, 1*, 6–12. https://doi.org/10.3969/j.issn.1002-9753.2013.01.002
18. Shengzu, G., & Min, W. (2012). Theoretical considerations and strategic choice on the development of smart city. *China Population, Resources and Environment, 22*(5), 74–80. https://doi.org10.3969j.issn1002-2104.2012.05.013
19. Sisi, T., Yanqiang, Z., Zhiguang, S., Wei, W., & Yaqi, Z. (2020). Wǒguó xīnxíng zhìhuì chéngshì fāzhǎn xiàn-zhuàng, xíngshì yǔ zhèngcè jiànyì [Development status, situation and policy suggestions of China's new smart cities]. *E-Government, 4*, 70–80. https://doi.org/10.16582/j.cnki.dzzw.2020.04.007
20. Vanolo, A. (2013). Smartmentality: The smart city as disciplinary strategy. *Urban Studies, 51*(5), 883–898. https://doi.org/10.1177%2F0042098013494427
21. Wei, F. (2016). Reconstruction of the path of personal information protection in the era of big data. *Global Law Review, 38*(5), 92–115. https://doi.org/10.3969/j.issn.1009-6728.2016.05.007
22. Xiao, S., & Jianfeng, C. (2017). Lùn réngōng zhìnéng de mínshì zérèn: Yǐ zìdòng jiàshǐ qìchē hé zhìnéng jīqìrén wéi qiērù diǎn [Civil liability of artificial intelligence: A perspective on autonomous vehicles and intelligent robots]. *Science of Law,* 35. https://www.ixueshu.com/h5/document/e9d0c5b740fa830675b85bc-07c8b6901318947a18e7f9386.html
23. Xibo, W., & Zaigao, Y. (2010). Zhìhuì chéngshì lǐniàn yǔ wèilái chéngshì fāzhǎn [The concept of smart city and future city development]. *Urban Studies, 17*(11), 56–60. https://doi.org/10.3969/j.issn.1006-3862.2010.11.009
24. Yuan, N. (2020). Jiànkāng mǎ yùnyòng zhōng de gèrén xìnxī bǎohù guīzhì [Regulation of personal information protection in health code application]. *Law Review, 38*(6), 111–121. https://doi.org/10.13415/j.cnki.fxpl.2020.06.012
25. Yujie, Z. (2017). Lùn réngōng zhìnéng shídài de jīqìrén quánlì jí qí fēngxiǎn guīzhì [Robot rights and risk regulation in the age of artificial intelligence]. *Oriental Law, 6*, 56–66. http://iolaw.org.cn/showNews.aspx?id=62222
26. Zhiwen, L. (2017). Réngōng zhìnéng chuàngzuò wù de zhùzuòquán bǎohù wèntí yánjiū [Legal protection of artificial intelligence creations]. *Science of Law, 35*(5), 156–165. http://gb.oversea.cnki.net/KCMS/detail/detailall.aspx?filename=1018874939.nh&dbcode=CMFD&dbname=CMFDREF

Information about the authors:

Bo Qin* — Ph.D., Professor, Head of the Department of Urban Planning and Management, Renmin University of China, Beijing, People's Republic of China.
qinbo@vip.sina.com

Su Qi — Master student, Department of Urban Planning and Management, Renmin University of China, Beijing, People's Republic of China.

Сведения об авторах:

Цинь Б.* — Ph.D., профессор, заведующий кафедрой городского планирования и управления Университета Жэньминь, Пекин, Китайская Народная Республика.
qinbo@vip.sina.com

Ци С. — студент магистратуры кафедры городского планирования и управления Университета Жэньминь, Пекин, Китайская Народная Республика.

https://doi.org/10.38044/2686-9136-2021-2-1-48-63

ARTICLES

DECENT WORK FOR DIGITAL PLATFORM WORKERS. A PRELIMINARY SURVEY IN BEIJING

Yan Xu[1], Dun Liu[2,*]

[1]School of Economics and Business Administration,
Beijing Normal University
19, Xinjiekouwai str., Haindian District, Beijing, People's Republic of China, 200044

[2]School of Economics and Management,
China University of Labor Relations
45, Zengguang rd., Haidian District, Beijing, People's Republic of China, 100048

Abstract

This paper discusses the status and implications of the employment relations and working conditions experienced by digital platform workers; the analysis is based on a survey conducted in 2017 on 1 338 workers engaged in work-on-demand via apps (WODVA) from 25 platforms in Beijing, of whom 48.8 % are full-time WODVA workers or take WODVA as their primary job. The survey finds that nearly a half of the respondents engage in platform work due to a lack of employment opportunities in formal labor markets or their permanent jobs providing insufficient income. The respondents reveal substantial decent work deficits in representation, compensation, job stability, social protection, working time, and health and safety: 1) WODVA workers seldom have any voice in labor dispute settlements and have a very low rate of unionization; 2) about one third of the full-time WODVA workers cannot earn a living wage and 7.6 % of them earn less than the minimum wage level; 3) three quarters of the full-time WODVA workers have no labor contract with the platforms or other employers, nor access to employer-contributed social insurances; 4) overtime work and underemployment coexist among full-time respondents, with nearly 10 % working for fewer than 4 hours per day while nearly 10 % work for more than 11 hours per day; 5) a majority of respondents run a higher risk of occupational health or physical risks, without any protection provided by the platforms or employers. To promote decent work by digital platform workers, the State needs to establish a portable social security system extending to all workers, to facilitate association and collective actions of platform workers either by extending the outreach of traditional unions or fostering new forms of organizations, to leverage digital technology to facilitate platform workers' organization and information sharing, and even to promote universal basic income and a workers' cooperative of platforms in the long run.

Keywords

digital labor platform, platform workers, work-on-demand via apps, decent work, working conditions, labor market regulation

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study is sponsored by the National Social Science Foundation of China (grant number: 16CJL036).

Acknowledgments The authors deeply appreciate Beijing Municipal Federation of Trade Unions (BMFTU) for their providing access to the datasets. The authors also express sincere gratitude to Professor Vladimir S. Osipov of the Moscow State Institute of International Relations for his selfless help in improvements and the publication of this article, along with other related scholars in Russia involved in cooperation with Beijing Jiaotong University under the grant of graduate education reform project of Beijing Jiaotong University "China-Russia Comparative Research in the Development of Labor Economics Discipline" (grant number: 134575522).

For citation Xu, Y., & Liu, D. (2021). Decent work for the digital platform workers. A preliminary survey in Beijing. *Digital Law Journal, 2*(1), 48–63. https://doi.org/10.38044/2686-9136-2021-2-1-48-63

* Corresponding author

Submitted: 24 Nov. 2020, accepted: 26 Jan. 2021, published: 31 Mar. 2021

СТАТЬИ

ОБЕСПЕЧЕНИЕ УСЛОВИЙ И ОХРАНЫ ТРУДА РАБОТНИКОВ IT-ПЛАТФОРМ В ПЕКИНЕ

Я. Сюй[1], Д. Лю[2,*]

[1]Школа экономики и делового администрирования,
Пекинский педагогический университет
200044, Китайская Народная Республика, Пекин, район Хайдянь,
ул. Синьцзекоувай, 19

[2]Школа экономики и менеджмента, Китайский университет
трудовых отношений
100048, Китайская Народная Республика, Пекин, район Хайдянь,
ш. Чжэнъян, 45

Аннотация

В статье обсуждаются условия труда работников цифровых платформ. Опрос 1 338 респондентов, занятых работой на 25 Интернет-платформах в Пекине (work-on-demand via apps, WODVA), показал, что почти половина из них работают на IT-платформах из-за отсутствия возможности трудоустройства на традиционном рынке труда или недостаточной заработной платы на основной работе. Респонденты отметили проблемы, связанные с невозможностью участия в деятельности профсоюзов, недостаточной заработной платой, отсутствием стабильности, социальной защищенности, а также проблемы регламентации рабочего времени, охраны труда и техники безопасности, а именно: 1) отсутствует эффективный механизм разрешения трудовых споров из-за недостаточной развитости профсоюзных организаций; 2) заработная плата около 1/3 опрошенных WODVA ниже прожиточного минимума, а 7,6 % — меньше минимального размера оплаты труда; 3) 3/4 работников WODVA, занятых полный рабочий день, не имеют трудового договора

с платформами или другими работодателями, а также доступа к социальному страхованию; 4) почти 10 % опрошенных работают более 11 часов в день, тогда как около 10 % заняты менее 4 часов в день; 5) у большинства респондентов отсутствуют гарантии по предоставлению медицинских услуг в связи с временной нетрудоспособностью из-за заболеваний. Государству необходимо распространить систему социального обеспечения на всех работников, в том числе занятых на IT-платформах, содействовать развитию профсоюзного движения с помощью традиционных либо современных способов, использовать цифровые технологии для оптимизации работы и обмена информацией. Более того, в долгосрочной перспективе государству необходимо установить минимальный размер заработной платы в рассматриваемой сфере.

Ключевые слова

цифровая платформа, IT-платформа, работа на Интернет-платформе, платформа удаленной работы, WODVA, достойные условия труда, регулирование рынка труда, регулирование новых форм труда

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование спонсируется Национальным фондом социальных наук Китая (номер гранта: 16CJL036).
Благодарность	Авторы глубоко признательны Пекинской муниципальной федерации профсоюзов (BMFTU) за предоставленный доступ к базам данных. Авторы также выражают искреннюю благодарность профессору МГИМО В. С. Осипову за его бескорыстную помощь в улучшении и публикации настоящей статьи, а также другим российским ученым, сотрудничавшим с Пекинским университетом Цзяотун в рамках гранта проекта реформы высшего образования Пекинского университета Цзяотун на тему «Китайско-российские сравнительные исследования в развитии дисциплины экономики труда» (номер гранта: 134575522).
Для цитирования	Сюй, Я., Лю, Д. (2021). Обеспечение условий и охраны труда работников IT-платформ в Пекине. *Цифровое право, 2*(1), 48–63. https://doi.org/10.38044/2686-9136-2021-2-1-48-63

* Автор, ответственный за переписку

Поступила: 24.11.2020; принята в печать: 26.01.2021; опубликована: 31.03.2021

Introduction

The last decade has seen the notable upsurge of digital labor platforms, making “gig work” a truly global phenomenon[1] (Gutbrod, 2020; Inozemtsev, 2020). According to the widespread definition, “digital platform work” can be grouped into two categories[2] (Menegatti, 2018). One is “crowd

[1] Zhou, I. (2020). *Digital labour platforms and labour protection in China*. International Labor Office. https://www.ilo.org/beijing/information-resources/WCMS_757923/lang--en/index.htm

[2] Codagnone, C., Abadie, F., & Biagi, F. (2016). The future of work in the “sharing economy”. Market efficiency and equitable opportunities or unfair precarisation? *JRC Science for Policy Report EUR 27913 EN*. http://doi.org/10.2791/431485; De Stefano, V. (2016). The rise of the “just-in-time workforce”: On-demand work, crowdwork and labour protection in the “gig-economy”. *Conditions of Work and Employment Series No. 71*. International Labor Office. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_443267.pdf

work", which is both managed and carried out online, either requiring more specialized skills such as logo design and software development (e. g. Freelancer.com, Upwork), or involving lower-skilled, repetitive "microtasks" such as data entry and content moderation (e. g. Amazon MTurk, Clickworker). The other is "work-on-demand via apps", which is managed online but carried out offline, mostly incorporating traditional services restricted to a local-based labor market, such as transportation (e. g. Uber, Lyft), delivery (e. g. Instacart, Deliveroo), and home services (e. g. Taskrabbit, Helpling). Although the size of the platform economy is still relatively modest (Farrell & Greig, 2016; Ilsøe, 2017), it is expanding at a remarkable pace. For example, a widely cited report predicts revenue in the key sectors of the platform economy growing from US $ 15 bn as of this date to US $ 335 bn in 2035;[3] an index measuring the utilization of digital labor platforms suggests their use is growing globally at a rate of 25 % per annum (Kässi & Lehdonvirta, 2018).

As the fastest-rising star of digital economy, China has emerged as a global leader in some key digital industries[4] (Liu et al., 2020), especially the sharing economy. According to the report issued by RCSE[5] in 2008, the sales revenue of the sharing economy in China amounted to 2942 billion RMB, at a growth rate of 41.6 % compared to the last year, involving 760 million participants and 75 million service providers; China accounts for 83 of the 305 "Unicorns" around the globe, among which 34 are players in the sharing economy. Digital labor platforms are the fastest-growing business in China's sharing economy. The major digital labor platforms include Didi Chuxing (DiDi) for ride-hailing, Eleme and Meituan for food delivery, ZBJ.com (Zhubajie) for professional consulting, 58.com for household services, ymm56.com for transportation, haodf.com for online consulting, and Homeincare for household medical care.[6] From 2015 to 2018, passenger volume of online ride-hailing increased from 9.5 % to 36.3 % of the overall taxi passenger volume; the revenue generated from food delivery expanded from 1.4 % to 10.6 % of the overall revenue of the catering sector.[7]

Although proponents argue that digital platforms can significantly facilitate meeting labor supply and demand, reduce transaction costs, enhance flexibility and autonomy for both providers and customers, and create jobs (especially for those socially marginalized groups)[8] (Johnston & Land-Kazlauskas, 2018), more and more scholars recognize its challenge to traditional employment relations and labor market regulation. Because digital platform workers are usually classified as self-employed or independent contractors, they are devoid of the fundamental rights and protection accessed by dependent employees, such as overtime compensation, minimum wage, social security, paid leave, and the ability to engage in collective action[9] (Aloisi, 2016; Sidorenko & von Arx, 2020; Sundararajan, 2016). It has been almost a consensus that, instead of a disruptive change to the labor

[3] PWC. (2015). *The sharing economy — Consumer intelligence series*. https://www.pwc.fr/fr/assets/files/pdf/2015/05/pwc_etude_sharing_economy.pdf

[4] Zhang, L., & Chen, S. (2019, January 17). *China's digital economy: Opportunities and risks*. International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459

[5] RCSE. (2019). Zhōngguó gòngxiǎng jīngjì fāzhǎn niándù bàogào [*Annual report of China's Sharing Economy Development*]. https://researchprofiles.herts.ac.uk/portal/en/publications/crowd-work-in-europe(30dbdc7c-9919-4150-a485-4fcb06cd6606)/export.html

[6] Zhou, 2020.

[7] RCSE, 2019.

[8] Huws, U., Spencer, N. H., & Joyce, S. (2016, December). *Crowd work in Europe: Preliminary results from a survey in the UK, Sweden, Germany, Austria and the Netherlands*. Foundation for European Progressive Studies. https://uhra.herts.ac.uk/bitstream/handle/2299/21934/crowd_work_in_europe_draft_report_last_version.pdf?sequence=1

[9] Berg, J., Furrer, M., Harmon, E., Rani, U., & Silberman, M. S. (2018). *Digital labour platforms and the future of work: Towards decent work in the online world*. Geneva: International Labor Office. https://www.ilo.org/global/publications/books/WCMS_645337/lang--en/index.htm; Huws et al., 2016; Berg et al., 2018.

markets, labor platform is nothing but the continuation of the broad shift toward more precarious and contingent labor as has lasted for several decades[10] (Aloisi, 2016; Menegatti, 2018). Ever since the early 1980s, globalization and neoliberal transformation has enabled capitalists to re-commodify labor by offshoring, outsourcing, and deploying non-standard labor contracts. In this context, the concept of decent work emerges as an institutional effort to combat the degradation of the labor market (Pereira et al., 2019). In 1999, the Director General's report presented to the 87th International Labor Conference declared: "The primary goal of the ILO today is to promote opportunities for women and men to obtain decent and productive work, in conditions of freedom, equity, security and human dignity".[11] Four strategic objectives were proposed to underpin the realization of this goal, namely, standards and fundamental principles and rights at work, employment, social protection, and social dialogue. From this perspective, digital labor platforms pose unprecedented challenge to the decent work agenda.

Although an increasing number of surveys on "crowd work" have emerged recently[12] (Graham, et al., 2017), surveys on "work-on-demand via apps" (WODVA) are quite scarce. A survey on WODVA is especially critical for China, given it constitutes a large proportion of China's sharing economy and given its prominent role in China's job creation in the post-crisis era. This article aims to reflect the decent work deficits experienced by digital platform workers based on a questionnaire survey of 1 338 WODVA workers in Beijing. To our knowledge, this is the first survey with a large sample size on WODVA conducted in China (which is also very scarce in other countries). Firstly, we present an overall description of the demographic distribution and employment status of the samples. Then, we dive into the working conditions of the respondents through the lens of the widely agreed decent work measurements, including fundamental rights at work, compensation, job stability, social security, working time and autonomy, health and safety, and career development. Finally, we discuss the policy and legislative implications to promote decent work of the digital platform workers.

Description of Data and Samples

Data Collection and Demographic Features

The survey was commissioned by Beijing Municipal Federation of Trade Unions (BMFTU) and conducted by the staff of BMFTU, in collaboration with a third-party research company, from March to May 2017. The survey covers 25 platforms clustered within 3 broad categories of business: namely, ride-hailing, logistics and express delivery, and household services. The questionnaires are distributed either by BMFTU staff when they made on-site interviews with the platform managers, or by the staff of the research company making face-to-face interviews with randomly selected WODVA workers on the street. A total of 1 400 questionnaires were distributed, with 1 338 effective samples collected. Specific on-demand jobs taken by the respondents include ride-hailing driver (46.2 %), housekeeper (12.2 %), courier (8.4 %), massagist (6.9 %), car wash (6.5 %), cooker (6.1 %), home repair (4.5 %), manicurist (4.1 %), legal / medical / tutor services (2.8 %), and house moving (2.2 %). The demographic composition of the samples is shown by Table 1.

[10] De Stefano, 2016; Berg et al., 2018.

[11] ILO. (1999). *Report of the Director-General: Decent work.* http://www.ilo.org/public/english/standards/relm/ilc/ilc87/rep-i.htm

[12] Zhou, 2020; Huws et al., 2016; Berg et al., 2018.

Table 1

The Demographic Composition of the Samples

Demography	Composition, (%)
Gender	male: 61.2; female: 38.8
Age	24 and below: 8.5; 25–34: 41.0; 35–44: 35.2; 45–54: 14.0; 55–64: 1.4
Household registration	local: 46.8; non-local with residence permit: 34.1; non-local without residence permit: 19.1
Education	junior high school: 24.6; high school or middle vocational school: 31.5; junior college or higher vocational school: 26.2; undergraduate: 14.3; graduate or higher: 3.4

Nearly 85 % of the respondents are less than 45 years old. This is consistent with the findings of other surveys that digital platform workers are dominated by young people[13] (Graham et al., 2017). The overall gender distribution is generally balanced, but it is quite uneven in different jobs. Male workers account for over 75 % of ride-hailing drivers, couriers, and home repairers, while female workers account for over 82 % of housekeepers and manicurists. Over half of the respondents have non-local household registrations (*Hukou*). Excluding ride-hailing drivers — among whom 60.4 % are local as the traffic administration authority in Beijing stipulated that ride-hailing drivers must be local residents (i. e. have Beijing *Hukou*) — 64.9 % of the respondents are non-local. This confirms that WODVA is more likely to be taken by marginalized workers, since non-local workers generally face inferior employment status under China's *Hukou* system. The distribution of education level is also quite uneven but as expected. Among the legal / medical / tutor service, 40.5 % have a bachelor's degree and 21.6 % have a master's degree; among the lower-skilled jobs, however, such as car wash, housekeeping, and couriers, 72.4 %, 54.6 %, and 31.3 % have an education level of only junior high school or even lower, respectively.

Employment Status and Motivation

43.0 % of the respondents take WODVA as their full-time job; an additional 5.8 % take WODVA as their major job while doing other part-time offline jobs; the remaining 51.2 % have their own permanent jobs. The proportion of full-time participants in WODVA found in this survey is much higher than the counterpart in crowd work as reported by other studies[14] (Graham et al., 2017; Ilsøe, 2017). 91.1 % of the respondents work for a single platform; 7.7 % work for two platforms; the final 1.2 % work for three or even more platforms. The percentage of working for two and more platforms is the highest (16.6 %) among those who take WODVA as their major job while doing other part-time offline jobs. This is not surprising, since their employment status implies that they are desperate to find more channels to increase their income.

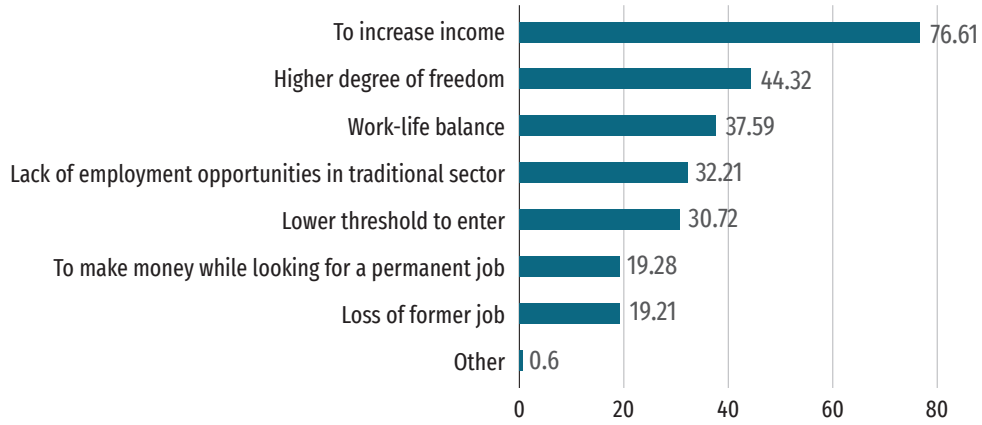
As for motivation to engage in WODVA, the distribution of the responses is shown in Figure 1. As expected, "to increase income" is the most frequently selected motivation, followed by "work-life balance" and "higher degree of freedom". 48.2 % of the respondents choose at least

[13] Zhou, 2020; Huws et al., 2016; Berg et al., 2018.

[14] Huws et al., 2016.

Figure 1

Distribution of Motivation to Engage in WODVA, (%)



one of the following motivations: "lack of employment opportunities in traditional sectors", "lower entry threshold", "loss of former job", and "to make money while looking for a permanent job". This means that nearly half of respondents do not engage in WODVA voluntarily, but simply because they could not find another acceptable permanent job. For those full-time WODVA workers or those who take WODVA as their primary job, this proportion increases to 58.6 %.

Working Conditions of WODVA Workers

The concept of decent work provides a comprehensive framework for evaluating the workers' working condition or employment quality, as well as an integrative policy agenda to promote the citizens' work-life wellness. It is particularly relevant to this study since it was proposed as a response to the increasing precariousness and informality of labor relations in the new global context. Numerous scholars and international organizations have contributed to the concepts and measurements of decent work, either using macro-level indicators (e. g. Anker et al., 2003; Bescond et al., 2003; Bonnet et al., 2003; Ghai, 2003) or micro-level scales (Duffy et al., 2017; Ferraro et al., 2018; Webster et al., 2015). Although scholars have not agreed upon a uniform set of measurements, they share many aspects in common with decent work, such as fundamental principles and rights at work (free from mistreatment, workers' representation, rights of collective action, etc.), adequate compensation, access to social security, employment safety, a safe work environment, decent working hours or a good work-life balance, fulfilling and meaningful work, and opportunities for personal development. Subject to the data collected, this study present the survey results of the working conditions of WODVA workers from the widely agreed aspects of decent work, including fundamental rights at work, compensation, job stability, social security, working time and autonomy, and health and safety.

Fundamental Rights at Work

Fundamental rights at work involve being treated with equity and dignity, worker's representation in decision making and disputes settlement, and freedom of association. Because a significant power asymmetry exists between workers and platforms, and platforms usually operate on behalf on the customers, the workers seldom have a say whenever there is dispute on the terms of trade. Typical examples are "wage theft" for crowd work (i.e. the customers can reject work without giving any reason) and the lack of dispute resolution policy if workers think they are rated unfairly (Schmidt, 2017). Our survey finds that 19.0 % of the respondents explicitly report that they have at some point had at least one dispute (if not more) with the platform (whilst another 10.4 % report "not clear"). By comparison, according to the 8th Survey on Status of Employees (SSE) in Beijing conducted by BMFTU in 2017, which generally covers those unionized, formal-sector employees, the proportion of employees who had had dispute(s) with employers are no more than 5.6 %.

For digital platform workers, the deficiency in fundamental rights at work which is most of concern is the inability to form an association. The inability to build any large-scale digital labor movement is especially obvious for crowd workers, "not only because many of them simply don't know each other, but also because there is an understanding that if they withdraw their labor, then workers in other parts of the world are able quickly to replace them". For WODVA participants, this problem may be alleviated, since they generally operate in local traditional labor markets; nevertheless this issue still remains, given their being classified as self-employed or independent contractors. Those unions already in existence have no experience — or even legitimacy — to mobilize them. Our survey shows that only 26.5 % of the respondents are union members. Actually, a majority of the union members are from those who have a permanent job; for full-time WODVA workers, only 20.8 % are union members.

Compensation

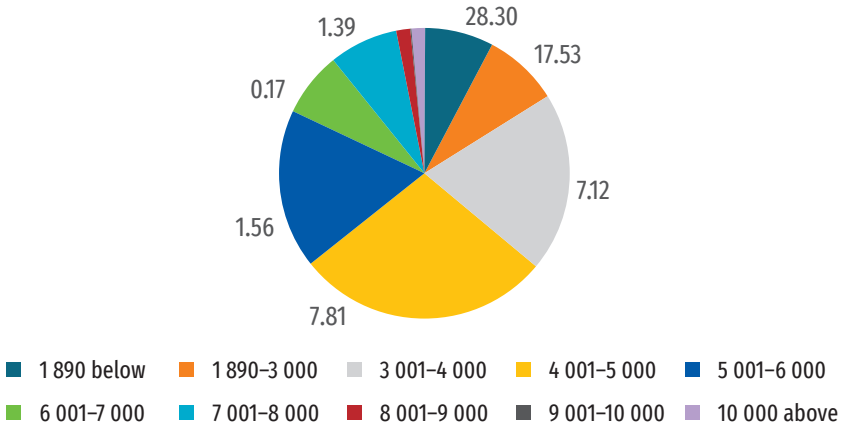
Economic uncertainty is a very likely condition for digital platform workers, given the fierce competition and lack of unionization[15] (Menegatti, 2018). Crowd workers are more likely to be obliged to accept low pay since the fierce competition often result in underbidding practices (Graham et al., 2017). WODVA workers are less likely to underbid their pay rate but face the same extent of income instability. When being asked "what are you most worried about in doing this work", 57.0 % and 51.64 % chose "income instability" and "instable flow of customers", respectively, ranking the most frequently chosen responses.

The distribution of monthly income level for full-time WODVA workers is shown in Figure 2. More than one third (36.1 %) earn less than 4 000 Yuan per month, which can hardly guarantee a decent living in Beijing, although according to the 8th SSE, this proportion is only 28.9 %. Particularly, 7.6 % of full-time WODVA workers earn a monthly income less than 1 890 Yuan, or the minimum wage level of Beijing in 2017. Low pay occurrence is especially common for those low skilled WODVA jobs, including housekeepers, couriers, house moving, and car washing, among which 42.6 % earn a monthly income of less than 4 000, and 9.1 % earn a monthly income of less than minimum wage level. In consideration of the lack of employers' contribution to social security and other benefits, the economic situation of WODVA workers are even worse than the data indicates compared to those formal-sector employees.

[15] De Stefano, 2016.

Figure 2

Distribution of Average Monthly Income of Full-Time WODVA Workers, (%)



Job Stability and Social Security

The most discussed issue related to digital platform work is the precariousness or the contingency of the jobs due to the classification of their employment status. In our survey, for those full-time WODVA workers or those who take WODVA as their major work, only 25.0 % report that they have signed labor contract with the platform; 40.4 % report that they have only signed a cooperation agreement with the platform; while 34.6 % claim that they have signed nothing with the platform. The lack of a labor contract leads to the lack of any social security, since only dependent employees who have a labor contract have access to social insurances partly contributed by employers. The survey shows that 34.4 % of the full-time WODVA workers or those who take WODVA as their major work have no access to social insurances. Among the remaining workers who have access, 40.8 % pay all the premium by themselves, 13.6 % share premium payment with their former employers, and only 11.2 % share premium payment with the platforms.

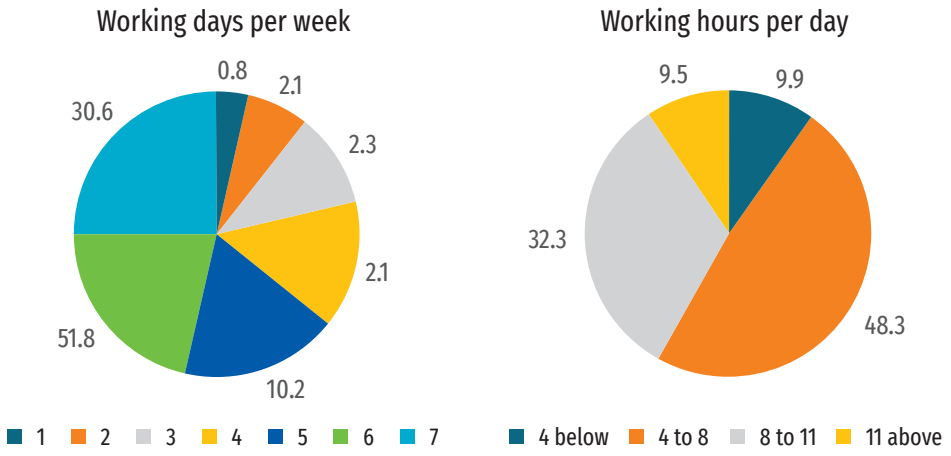
Working Time and Autonomy

A work schedule with greater flexibility is an important reason for many workers who participate in WODVA. However, "flexibility is just a kind of solace: to earn a significant sum of money, workers might also have to work more hours every day than a 'standard' worker. Since they have to be available 'around the clock', this kind of flexibility does not entail a greater freedom for the worker". Figure 3 displays the distribution of working time of full-time WODVA workers. An overwhelming majority (82.4 %) of the respondents have no weekends; 41.8 % of the respondents work for more than 8 hours per day; and 9.5 % even work for more than 11 hours. Furthermore, overwork coexists with a considerable amount of underemployment, implying that, given the highly instable demands and low pay rates, WODVA workers are desperate to work for more time to earn sufficient income. This is consistent with Berg's[16] finding that the majority of crowd workers would prefer to work more, but are hindered by limited available tasks.

[16] Berg et al., 2018.

Figure 3

Distribution of Working Time of the Full-Time WODVA Workers, (%)



Neither do WODVA worker enjoy a true sense of autonomy in way of work, since they are under the close control of the platforms' algorithm-driven rating system[17] (Aloisi, 2016; Schmidt, 2017). 64.9 % of the respondents explicitly report that the platforms have some evaluation and incentive system, and 9.8 % report "not clear". As shown by Figure 4, the respondents confirm that the platforms have requirements for multiple aspects of their work, among which the service quality, service language, online time, and order quantity rank the highest in proportion of confirming responses. 86.7 % of the respondents confirm requirements on at least four aspects. This reality refutes the platforms' assertion that WODVA workers are self-employed or independent contractors. Majority of them are *de facto* employees of the platforms, given what close control platforms clearly have of their workers' labor processes.

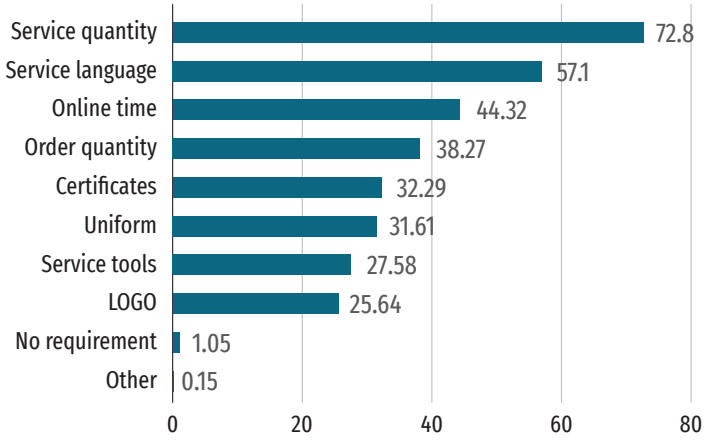
Health and Safety

By shirking an employment relationship with the workers, the companies (as well as the platforms) externalize obligations and the ensuing costs of preventing health and safety hazards befalling individual workers. The popular WODVA jobs are characterized by salient health and safety hazards, such as traffic accidents, exposure to chemicals, carrying heavy loads, or working at heights or various uneasy environments. These hazards are aggravated when workers are desperate to undertake more orders within a given time. Nowadays, a hot-button issue in China is that food delivery couriers are becoming the most visible victims as well as instigators of traffic accidents, because they have to drive (usually motorbikes) as fast as they can within a very harsh time limit, given that being late leads to a severe penalty on remuneration and their personal rating. As a food delivery rider said in a widely watched blog entitled *Food Delivery Riders Trapped in System* published in September 2020, "the riders are racing against death, struggling with the traffic police, and making friends with the red lights". This blog lists the following data which was cited from traffic police corps in several cities: during the first half of 2017 in Shanghai, there was one food delivery rider

[17] Berg et al., 2018.

Figure 4

Proportion of Confirming Responses to the Platforms' Working Requirements, (%)



casualty every 2.5 days; in 3 months of the same year, 12 casualties of food delivery riders happened in Shenzhen; in 7 months of 2018 in Chengdu, the traffic police handled 196 accidents related to food delivery riders, with 155 casualties, or one casualty per day, due to the riders' traffic offences. According to our survey, only 13.9 % of respondents confirm that platforms provide labor protection appliances, and 48.6 % report that the issue most worrying them is "traffic, personal assault, working injury or other fortuitous accidents", ranking as the third most frequently chosen issue following "income instability" and "unstable flow of customers".

Implications for Promoting Decent Work for Digital Platform Workers

Given most operational labor market regulations are applied to dependent employees, many scholars and practitioners have discussed reclassifying the employment status of digital platform workers. In recent years, several class action lawsuits have been brought against Uber, Lyft, and Crowdflower, to challenge the platforms' classifications (Cherry, 2016; Johnston & Land-Kazlauskas, 2018). These struggles have borne some fruits. For example, the US district court in the north district of California and the labor commissioner of the State of California, in three separate cases against Uber and Lyft, recognized that a driver was an employee of Uber or Lyft instead of being self-employed.[18] On January 1st, 2020, California passed the AB5 act, which stipulates that a workers could not be classified as independent contractor unless the employer could prove that (a) the working performance of the employed is not under the control and direction of the employer, (b) the work done by the employed is not the normal business of the employer, or (c) the employed usually participates in transactions, operations, or practices independently. According to this act, drivers of Uber and Lyft and workers on many other WODVA platforms will be classified as employees. Long before that, some companies, such as

[18] De Stefano, 2016.

Alfred, Instacart, and Munchery, have indeed already spontaneously reclassified a part of their workers as employees.[19]

In our opinion, instead of debating whether platform workers are "employees" or even proposing an intermediary category of classification[20] (Todolí-Signes, 2017), a more fundamental and feasible solution is to reform the traditional labor market regulation system so as to extend the labor rights protection to all kinds of workers (Graham et al., 2017; Menegatti, 2018; Sundararajan, 2016). This proposition is innate within the ILO's primary objective of "decent work for all".[21] A new safety net should be built by making the social security "universal" and "portable"; that is, instead of the employers' direct contribution of social security, a tax-financed, universally covered social security should be provided by the states. This model has long been adopted by the Scandinavian countries, based on the concept of "flexicurity" (a linguistic combination of "flexibility" and "security"). Besides, other labor rights accessed by dependent employees, such as minimum wage and working time limits, should also be extended to the non-standard labor relations. In the long run, nonetheless, a universal basic income may be a more fundamental and socially desirable solution (Pulkka, 2017; Sundararajan, 2016).

Another indispensable solution to promote decent platform work is to support platform workers with their association and labor movement. This is pivotal to make a level playing field given the huge power asymmetry between platforms and workers. Existing unions can lend powerful support to the labor movement of platform workers by extending membership to non-standard workers, giving legal advice, providing group policies of insurances, carrying on public relations campaigns, mobilizing collective actions, or even helping to cultivate union-like organizations. Within Europe, many unions have a long history of incorporating non-standard workers into their ranks. In Italy, for instance, unions created specific representational opportunities in existing labor confederations for non-standard workers (Pulignano et al., 2015). In many parts of the world, there has been an emergence of rejuvenated or even completely new collective organizations, such as the Spanish workers' collective and informal associations, solidarity movements like the broodfonds in the Netherlands, the Independent Drivers Guild in New York, and the Independent Workers Union in Great Britain, and other initiatives aimed at helping or supporting the collective organization of platform workers.[22] One of the best-known examples is the Independent Workers Union in Great Britain (IWGB), which was formed explicitly to organize non-traditional, low wage, and immigrant workers. Its successes include supporting the couriers' strike in protesting Deliveroo (a food delivery platform) to reduce the pay rate in August 2016 (Johnston & Land-Kazlauskas, 2018). In China, given its centralized union system, the official unions should take more responsibility in organizing platform workers or should even act as the negotiators. For instance, the Beijing Express Delivery Association and the Beijing Express Delivery Workers' Federation organized enterprises and workers' representatives in early 2019 to sign China's first Special Collective Contract for Labor Protection in the express delivery industry, and agreed on setting up labor protection inspectors and purchasing accidental injury insurance for workers[23].

---

19 De Stefano, 2016.

20 Weber, L. (2015, January 28). *What if there were a new type of worker: Dependent contractor*. Wall Street Journal. http://www.wsj.com/articles/what-if-there-were-a-new-type-of-worker-dependent-contractor-1422405831

21 ILO, 1999.

22 Daugareilh, I., Degryse, C., & Pochet, P. (Eds.). (2019). The platform economy and social law: Key issues in comparative perspective. ETUI Research Paper — Working Paper 2019.10. Brussels: ETUI. http://doi.org/10.2139/ssrn.3432441

23 Zhou, 2020.

While platform workers can be hard to organize, network technology provides convenient conditions for their communication.[24] As Degryse[25] clarified, "the trade union movement could perhaps discover in these new technologies an additional tool for exchange, cooperation, mobilization, action, visibility, etc." Platform workers are spontaneously establishing Internet tools such as FairCrowdwork.com and turkernation.com, creating grassroots, democratic, worker-driven forums in which platform workers meet virtually and exchange information (Fabo et al., 2017). Such online forums are not only potential trade union allies, but also provide workers with the ability to rate platforms or clients and critique their actions, and hence intensify competition between platforms via the reputation mechanism.

Finally, few organizational models promote worker voice and control more than cooperatives, where workers are both owners and participants in the operation of the enterprises (Johnston & Land-Kazlauskas, 2018). If labor movements leveraged by platform technology are "digitalization used by workers", then platform cooperatives are "digitalization owned by workers". Initiated and promoted by Trebor Scholz, professor at the New School in New York, the "platform cooperativism" movement advocates a new platform type based on cooperative ownership (Scholz, 2016, 2017). By building and owning the platforms themselves, the workers can redesign working conditions from bottom up, "so as to crack the broken system of the sharing economy / on-demand economy that only benefits a few" (Scholz, 2017). The taxi industry has given rise to a number of new cooperative firms in recent years. Swift may be an early example of a platform owned by drivers. A different yet familiar idea — allocating shares of platforms (that remain shareholder corporations) to providers — seems like the most pragmatic near-term path towards sharing the wealth of the sharing economy. An early example of this kind of program is Juno, a ridesharing service that has committed to ensuring that its drivers own 50 % of the company's founding stock by 2026 (Sundararajan, 2016).

Conclusion

As an advanced variant of neoliberal capitalism, digital labor platforms have posed an unprecedented challenge to the decent work agenda. China's leading role in the development of the sharing economy (especially the WODVA form) makes China a representative research target of digital platform and its implications on the labor market. This study presents a micro-level survey on the employment status and working conditions of 1 338 WODVA workers from 25 platforms in Beijing. The survey confirms the role of digital platforms in job creation, especially for those with less employability, and in providing complementary income other than permanent jobs. However, nearly a half of them engage in WODVA due to a lack of employment opportunities in standard labor markets. The respondents show multiple decent work deficits, reflected by a lack of representation and organization, low pay rates and hence inadequate compensation, income and job instability, insufficient accesses to employer-contributed social security, overtime work, and high exposure to physical and health hazards. These results are consistent with the existing studies on crowd workers. To promote decent work of digital platform workers, the State needs substantial reform in its labor market regulation, including extending social security and labor rights protection to all workers, promoting association and collective actions of platform workers either by

[24] Degryse, C. (2016). Digitalisation of the economy and its impact on labour markets. ETUI Research Paper — Working Paper 2016.02. Brussels: ETUI. http://doi.org/10.2139/ssrn.2730550

[25] Degryse, C. (2016). Digitalisation of the economy and its impact on labour markets. *ETUI Research Paper — Working Paper 2016.02*. http://doi.org/10.2139/ssrn.2730550

extending traditional union's outreach or fostering new forms of organizations, and leveraging platform technology to facilitate platform workers' organization and information sharing. In the long run, a universal basic income and public ownership will be the more fundamental solution to guarantee decent work lives in the digital economy.

This study is valuable in that it is the first survey on WODVA workers with a large sample size. Its implications for labor market regulation is particularly relevant to China, since the Chinese government, with a long tradition of developmentalism, has taken an approach that does not overly regulate but instead promotes — and even hails — the development of digital labor platforms. Despite its originality and relevance, this study is quite preliminary given its scope and depth are constrained by the dataset provided by BMFTU. To attain more in-depth and extensive insights into the working conditions of platform workers and their implications, we suggest the following improvements in data collection: (a) variables and the corresponding data types should be made consistent with the existing mainstream micro datasets in China, such as Survey on Status of Employees (SSE), Dynamic Survey on Labor Markets (DSLM), and Urban Household Survey (UHS), so as to better delineate the decent work gaps of platform workers in comparison with those in formal sectors; (b) datatypes related to compensation and working time should be more precise (instead of the rough interval distribution presented in this survey), so that the pay rates could be evaluated more specifically; (c) a more detailed survey on employment status and motivation should be made to both full-time and part-time platform workers (e.g. for full-time platform workers: whether the respondents engage in platform work due to a loss of permanent job, whether they are actively looking for a permanent job, the income level and working time of their former permanent job, etc.), so that researchers can find out which groups of workers are more likely to engage in platform work, whether they do so voluntarily or just because of limited access to formal sectors or/and their permanent job's failing to provide a living wage, and to what extent the platforms contribute to "net" job creation or just replace those traditional jobs destroyed by digitalization; (d) more variables should be added to reflect the determinants and outcomes of the working conditions. The latter includes, for instances, the physical and mental wellness of the respondents, the level and structure of their expenditure, and the savings and indebtedness of the households, which are crucial to evaluate the micro-, macro-, and socio-economic consequences of the precariousness caused by digitalization.

References:

1. Aloisi, A. (2016). Commoditized workers. Case study research on labour law issues arising from a set of "on-demand / gig economy" platforms. *Comparative Labor Law & Policy Journal, 37*(3), 653–687. http://doi.org/10.2139/ssrn.2637485
2. Anker, R., Chernyshev, I., Egger, P., Mehran, F., & Ritter, J. A. (2003). Measuring decent work with statistical indicators. *International Labour Review, 142*(2), 147–178. http://doi.org/10.1111/j.1564-913X.2003.tb00257.x
3. Bescond, D., Châtaignier, A., & Mehran, F. (2003). Seven indicators to measure decent work: An international comparison. *International Labour Review, 142*(2), 179–212. http://doi.org/10.1111/j.1564-913X.2003.tb00258.x
4. Bonnet, F., Figueiredo, J. B., & Standing, G. (2003). A family of decent work indexes. *International Labour Review, 142*(2), 213–238. http://doi.org/10.1111/j.1564-913X.2003.tb00259.x
5. Cherry, M. A. (2016). Beyond misclassification: The digital transformation of work. *Comparative Labor Law & Policy Journal, 37*(3), 544–577. https://ssrn.com/abstract=2734288

6. Duffy, R. D., Allan, B. A., England, J. W., Blustein, D. L., Autin, K. L., Douglass, R. P., Ferreira, J., & Santos, E. J. R. (2017). The development and initial validation of the decent work scale. *Journal of Counseling Psychology, 64*(2), 206–221. http://doi.org/10.1037/cou0000191
7. Fabo, B., Karanovic, J., & Dukova, K. (2017). In search of an adequate European policy response to the platform economy. *Transfer: European Review of Labour and Research, 23*(2), 163–175. http://doi.org/10.1177/1024258916688861
8. Farrell, D., & Greig, F. (2016). Paychecks, paydays, and the online platform economy: Big data on income volatility. *Proceedings. Annual Conference on Taxation and Minutes of the Annual Meeting of the National Tax Association, 109,* 1–40.
9. Ferraro, T., Pais, L., Rebelo Dos Santos, N., & Moreira, J. M. (2018). The decent work questionnaire: Development and validation in two samples of knowledge workers. *International Labour Review, 157*(2), 243–265. http://doi.org/10.1111/ilr.12039
10. Ghai, D. (2003). Decent work: Concept and indicators. *International Labour Review, 142*(2), 113–145. http://doi.org/10.1111/j.1564-913X.2003.tb00256.x
11. Graham, M., Hjorth, I., & Lehdonvirta, V. (2017). Digital labour and development: Impacts of global digital labour platforms and the gig economy on worker livelihoods. *Transfer: European Review of Labour and Research, 23*(2), 135–162. http://doi.org/10.1177/1024258916687250
12. Gutbrod, M. (2020). Digital transformation in economy and law. *Digital Law Journal, 1*(1), 12–23. https://doi.org/10.38044/DLJ-2020-1-1-12-23
13. Ilsøe, A. (2017). The digitalisation of service work — Social partner responses in Denmark, Sweden and Germany. *Transfer: European Review of Labour and Research, 23*(3), 333–348. http://doi.org/10.1177/1024258917702274
14. Inozemtsev, M. I. (2020). Digital law journal: Introduction. *Digital Law Journal, 1*(1), 8–11. https://doi.org/10.38044/DLJ-2020-1-1-8-11
15. Johnston, H., & Land-Kazlauskas, C. (2018). *Organizing on-demand: Representation, voic, and collective bargaining in the gig economy*. *Conditions of Work and Employment Series No. 94.* Geneve: International Labour Office. http://www2.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_624286.pdf
16. Kässi, O., & Lehdonvirta, V. (2018). Online labour index: Measuring the online gig economy for policy and research. *Technological Forecasting and Social Change, 137,* 241–248. https://doi.org/10.1016/j.techfore.2018.07.056
17. Liu, D., Geng, Y., & Yuan, L.-Q. (2020). The age of digitalization: Tendencies of the labor market. *Digital Law Journal, 1*(3), 14–20. https://doi.org/10.38044/2686-9136-2020-1-3-14-20
18. Menegatti, E. (2018). A fair wage for workers on-demand via app. In E. Ales, Y. Curzi, T. Fabbri, O. Rymkevich, I. Senatori, & G. Solinas (Eds.), *Working in digital and smart organizations* (pp. 67-92). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-77329-2
19. Pereira, S., Dos Santos, N., & Pais, L. (2019). Empirical research on decent work: A literature review. *Scandinavian Journal of Work and Organizational Psychology, 4*(1), 1–15. https://doi.org/10.16993/sjwop.53
20. Pulignano, V., Ortíz Gervasi, L., & de Franceschi, F. (2015). Union responses to precarious workers: Italy and Spain compared. *European Journal of Industrial Relations, 22*(1), 39–55. https://doi.org/10.1177/0959680115621410
21. Pulkka, V.-V. (2017). A free lunch with robots — Can a basic income stabilise the digital economy? *Transfer: European Review of Labour and Research, 23*(3), 295–311. https://doi.org/10.1177/1024258917708704
22. Schmidt, F. A. (2017). *Crowd design: From tools for empowerment to platform capitalism*. Birkhäuser.
23. Scholz, T. (2016). *Platform cooperativism: Challenging the corporate sharing economy*. Rosa Luxemburg Stiftung. New York Office. https://rosalux.nyc/wp-content/uploads/2020/11/RLS-NYC_platformcoop.pdf
24. Scholz, T. (2017). *Uberworked and underpaid: How workers are disrupting the digital economy*. Polity Press.

25. Sidorenko E. L., & von Arx P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. *Digital Law Journal, 1*(1), 24–38. https://doi.org/10.38044/DLJ-2020-1-1-24-38
26. Sundararajan, A. (2016). *The sharing economy. The end of employment and the rise of crowd-based capitalism*. MIT Press.
27. Todolí-Signes, A. (2017). The "gig economy": Employee, self-employed or the need for a special employment regulation? *Transfer: European Review of Labour and Research, 23*(2), 193–205. https://doi.org/10.1177/1024258917701381
28. Webster, E., Budlender, D., & Orkin, M. (2015). Developing a diagnostic tool and policy instrument for the realization of decent work. *International Labour Review, 154*(2), 123–145. https://doi.org/10.1111/j.1564-913X.2015.00017.x

Information about the authors:

Yan Xu — Ph.D. in Economics, Professor, School of Economics and Business Administration, Beijing Normal University, Beijing, People's Republic of China.
ORCID 0000-0002-0612-1642

Dun Liu* — Ph.D. in Economics, Lecturer of School of Economics and Management, China University of Labor Relations, Beijing, People's Republic of China.
liudun@bjtu.edu.cn
ORCID 0000-0002-3977-6645

Сведения об авторах:

Сюй Я. — Ph.D. in Economics, профессор Школы экономики и делового администрирования Пекинского педагогического университета, Пекин, Китайская Народная Республика.
ORCID 0000-0002-0612-1642

Лю Д.* — Ph.D. in Economics, преподаватель факультета экономики труда Школы экономики и менеджмента Пекинского университета Цзяотун, Пекин, Китайская Народная Республика.
liudun@bjtu.edu.cn
ORCID 0000-0002-3977-6645

https://doi.org/10.38044/2686-9136-2021-2-1-64-82

СТАТЬИ

МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО В КИБЕРПРОСТРАНСТВЕ: RATIONE MATERIAE, RATIONE TEMPORIS И ПРОБЛЕМА КВАЛИФИКАЦИИ КИБЕРАТАК

С.Ю. Гаркуша-Божко

Школа высшего спортивного мастерства
по водным видам спорта имени Ю. С. Тюкалова
197110, Россия, Санкт-Петербург, Набережная Гребного канала, 10, стр. 1

Аннотация

Целью статьи является анализ таких проблем применения норм международного гуманитарного права (МГП) в киберпространстве, как проблема *ratione materiae* и *ratione temporis* данной отрасли международного публичного права в киберпространстве. Актуальность исследования подтверждается стремительным развитием информационных технологий, которые могут быть использованы в ходе вооруженного конфликта. Факт наличия «Таллиннского руководства 2.0» по международному праву, применимому к кибероперациям, также служит подтверждением актуальности настоящей темы. Использование сторонами вооруженного конфликта в киберпространстве новых технологий никак не влияет на применимость к таким военным действиям норм МГП. Какие именно кибероперации являются предметом регулирования права кибернетических вооруженных конфликтов? Этот вопрос, по нашему мнению, является ключевым. При этом киберпространство представляет собой не совсем обычный театр войны, поскольку средства и методы ведения военных действий никак не связаны с традиционным применением вооруженной силы. В статье уделяется внимание двум основным точкам зрения в отношении этой проблемы. В результате проведенного исследования автор приходит к выводу о том, что при всей очевидности теоретических выводов в отношении анализируемых проблем, они все равно не представляются всеобъемлющими в силу отсутствия соответствующей практики государств, которую необходимо развивать.

Ключевые слова

международное гуманитарное право, вооруженный конфликт, киберпространство, военные действия, кибероперации, кибератака, нападение, Таллиннское Руководство

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.

Для цитирования Гаркуша-Божко, С. Ю. (2021). Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак. *Цифровое право, 2*(1), 64–82. https://doi.org/10.38044/2686-9136-2021-2-1-64-82

Поступила: 23.12.2020; принята в печать: 19.02.2021; опубликована: 31.03.2021

ARTICLES

INTERNATIONAL HUMANITARIAN LAW IN CYBERSPACE: RATIONE MATERIAE, RATIONE TEMPORIS AND THE PROBLEM OF CYBER-ATTACK QUALIFICATION

Sergey Y. Garkusha-Bozhko

School of Higher Sportsmanship in Water Sports
named after Y. S. Tyukalov
1-10, Naberezhnaya Grebnogo Canala, St. Petersburg, Russia, 197110

Abstract

The purpose of the article is to analyse problems arising from applying the rules of International Humanitarian Law in cyberspace, particularly the problems of *ratione materiae* and *ratione temporis* of this branch of Public International Law in cyberspace. The rapid development of cyber technologies that can be used within an armed conflict affirm the applicability of this research. The existence of "The Tallinn Manual 2.0" on International Law Applicable to Cyber Operations also confirms the impact of this topic on the modern world. The fact that parties in armed conflicts use new technologies in cyberspace does not affect the applicability of IHL rules to such military actions. In the context of this issue, a key question which instigates scientific discussion is that of which cyber operations are subject to the regulation of the law of cyber armed conflicts. The urgent need to study this problem stems from the fact that cyberspace is not an ordinary theatre of war, with the means and methods of warfare used in it being in no way related to the traditional use of armed force; given this quality of cyber operations, it is essential to understand which areas may be subject to IHL. The article analyses two main doctrinal points of view in relation to this problem; as this doctrine (in the context of this issue) also addresses the legal qualification of cyber-attacks, the article also raises this topical issue. Based on the results of this analysis, the author concludes that, despite all the evidence of theoretical conclusions regarding the problems under analysis, they still do not seem comprehensive due to the lack of relevant state practice, which needs to be developed.

Keywords

International Humanitarian Law, armed conflict, cyberspace, hostilities, cyber-operations, cyber-attack, attack, Tallinn Manual

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Garkusha-Bozhko, S. Y. (2021). International humanitarian law in cyberspace: Ratione materiae, ratione temporis and problem of cyber-attack qualification. *Digital Law Journal, 2*(1), 64–82. https://doi.org/10.38044/2686-9136-2021-2-1-64-82

Submitted: 23 Dec. 2020, accepted: 19 Feb. 2021, published: 31 Mar. 2021

Введение

Развитие информационных технологий в наше время затрагивает все сферы деятельности человечества в мировом масштабе. Не стала исключением и сфера военной деятельности государств. На настоящий момент уровень развития военных информационных технологий позволяет говорить о возможности распространения военных действий на информационное пространство, или как его еще называют киберпространство (англ. *cyberspace*). Иными словами, в современном мире вооруженный конфликт в киберпространстве перестал быть выдумкой писателей-фантастов и сценаристов фантастических развлекательных фильмов — теперь это потенциально возможный конфликт, который может начаться из-за столкновения интересов двух и более государств в киберсфере. Вероятность такого конфликта также подтверждает заявление Президента России В. В. Путина, который отметил, что «одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере»[1].

Как отмечают в доктрине (Melzer, 2017), киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств. Данное утверждение не может быть оспорено по той причине, что в силу уровня развития современных технологий киберпространство, в действительности, является потенциальным театром военных действий. Высокая вероятность таких вооруженных конфликтов заставила государства задуматься об их правовом регулировании, и в 2013 году благодаря усилиям юристов и военных специалистов из стран военно-политического блока НАТО, при участии специалистов из Международного Комитета Красного Креста (МККК), было разработано «Таллиннское руководство по международному праву, применимому к кибервооружениям» (англ. "*Tallinn Manual on the International Law Applicable to Cyber Warfare*") (далее — Руководство) (Schmitt, 2013).

Руководство является попыткой разработать нормы международного права, применимые не только к такому роду вооруженных конфликтов, но и к киберпространству в целом, как в военное, так и в мирное время. Необходимость международно-правовых норм в этой области очень высока, что и обусловило принятие новой расширенной версии Руководства в 2017 г. Его существование лишний раз доказывает актуальность как проблемы правового регулирования вооруженных конфликтов в киберпространстве, так и проблемы правового регулирования киберпространства в целом.

[1] Путин, В. В. (2020, сентябрь 25). *Заявление о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности*. Официальный сайт Президента РФ. http://kremlin.ru/events/president/news/64086

Факт использования сторонами вооруженного конфликта в ходе военных действий в киберпространстве новых технологий никак не влияет на применимость к таким действиям норм международного гуманитарного права (МГП). Тем не менее, в силу различных особенностей киберпространства, в частности, анонимности его пользователей, при применении к кибернетическим военным действиям норм МГП возникает ряд проблем. Одной из которых, является вопрос о том, какие именно кибероперации становятся предметом регулирования права кибернетических вооруженных конфликтов? Иными словами, речь идет о *ratione materiae* МГП в киберпространстве. Эта проблема является предметом активных научных дебатов (Droege, 2012; Backstrom & Henderson, 2012; Schmitt, 2017; Zhang, 2012; Schmitt, 2002).

Ключевым моментом для применения норм международного гуманитарного права к киберпространству считается наличие фактической ситуации вооруженного конфликта в киберпространстве. Однако важно понимать, какие именно кибероперации будут регулироваться такими нормами, поскольку понимание обеспечивает соблюдение норм МГП в киберпространстве.

Причины необходимости исследования вопроса *ratione materiae* международного гуманитарного права в киберпространстве достаточно просты: киберпространство представляет собой не совсем обычный театр войны, т. к. средства и методы ведения военных действий, применяемых в нем, никак не связаны с традиционным применением вооруженной силы. Большинство кибероперaций направлено на длительное воздействие на объект кибернетического нападения с целью нарушения его нормального функционирования, но последствия такого негативного воздействия редко приводят к физическому разрушению или повреждению, что происходит в ходе традиционного вооруженного конфликта. Исходя из такой природы кибероперaций, крайне важно понять, какие из них могут являться предметом МГП. Особенно важно это понять в отношении кибероперaций, которые могут затронуть лиц, находящихся под защитой норм «права Женевы» — в первую очередь, это касается вопросов защиты гражданского населения. В современных условиях большинство информационных систем все-таки имеет гражданский характер, поэтому достаточно легко представить сценарии кибернетического вооруженного конфликта, в которых будет затронуто гражданское население.

Привести примеры ситуаций, в которых кибероперации будут затрагивать гражданское население, достаточно легко; причем они вызывают вопросы правовой квалификации, как в военное время, так и в мирное. К примеру, осуществление кибероперации, направленной на нарушение функционирования гражданской энергетической системы или системы водоснабжения без их физического разрушения.

Также можно привести пример компьютерного вируса *Stuxnet*, который имел своей целью нарушение нормального функционирования завода по обогащению урана в Исламской Республике Иран, в городе Нетензе. Настоящий пример является одним из ярчайших примеров длительного враждебного воздействия на соответствующие государственные информационные системы. Как было установлено, данный вирус был разработан при участии экспертов из спецслужб США и Израиля, и его целью была ядерная программа Ирана[2].

Государства, в частности, Иран, не квалифицировали ситуацию с вирусом *Stuxnet* в качестве нападения. Несмотря на это обстоятельство в доктрине была высказана мысль, согласно которой международный вооруженный конфликт в киберпространстве возникает, когда возможно установить конкретное государство, разработавшее вирус (Schmitt, 2012; Brown, 2011).

[2] Nakashima, E., & Warrick, J. (2012, June 1). *Stuxnet was work of U.S. and Israeli experts, officials say*. The Washington Post. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Так, G. D. Brown (2011) прямо заявляет, что вирус *Stuxnet* является кибератакой, возможно, в нарушение основополагающего международно-правового принципа неприменения силы и угрозы ею, а также в нарушение норм *jus in bello*. Исходя из таких заявлений в доктрине, вполне может возникнуть мысль о возможных кибератаках, осуществляемых неправительственной группой против правительства того или иного государства, что повлечет за собой вопрос о квалификации такого случая в качестве немеждународного вооруженного конфликта в киберпространстве.

Приведем другой пример ситуации, в отношении которой также звучали призывы к квалификации совершенных кибератак в качестве актов «кибервойны». Речь идет о кибератаках, совершенных против правительственных и банковских инфраструктур в Эстонии в 2007 году, в результате которых, в том числе, гражданские лица — клиенты пострадавших эстонских банков лишились доступа к банковским услугам (Tikk et al., 2010; Buchan, 2012; Pool, 2013)[3]. Многие журналисты, а также некоторые юристы из западных стран, основываясь на том, что данные кибератаки были совершены после принятия решения о переносе Бронзового солдата, необоснованно обвинили в этих кибератаках Российскую Федерацию (Tikk et al., 2010; Buchan, 2012; Pool, 2013)[4], хотя эксперты доказали непричастность Российской Федерации к этим кибератакам[5]. Мы не будем углубляться в эти споры, которые являются больше политическими, чем юридическими. Отметим только, что данный пример очень хорошо иллюстрирует необходимость определения *ratione materiae* международного гуманитарного права в киберпространстве.

Исходя из вышеперечисленного, мы поставим следующие вопросы. Во-первых, применяются ли нормы международного гуманитарного права только к кибероперациям, которые можно признать нападением, или ко всем военным кибероперациям, и с какого момента такие нормы будут применяться к таким операциям? В этой связи надлежит рассмотреть не только критерий *ratione materiae*, но и *ratione temporis*. Во-вторых, необходимо понять, что такое нападение (кибератака) в киберпространстве? Но перед исследованием вышеуказанных вопросов важно также ответить на вопрос, что такое киберпространство, с чего и начнется настоящее исследование.

Понятие киберпространства

Несмотря на стремительное развитие информационных технологий, на международном уровне до сих пор нет универсального определения киберпространства, а существует множество определений, закрепленных в различных международных документах.

Так, в статье 2 концепции Конвенции об обеспечении международной информационной безопасности, вынесенной Российской Федерацией в 2011 г. на рассмотрение в Организацию Объединенных Наций (ООН), под информационным пространством понимается сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием,

[3] См. также: Санжиев, А. (2007, июнь 7). *Таллин пошел по миру*. Российская газета. https://rg.ru/2007/06/07/estoniya.html; Орлов, А. (2007, июнь 6). *Атака хакеров на Эстонию шла не из России, а со всего мира — эксперт*. РИА Новости. https://ria.ru/20070606/66760771.html; Vitkine, B. (2017, Mars 14). L'Estonie, première cybervictime de Moscou [Estonia, Moscow's first cybervictime]. Le Monde. https://www.lemonde.fr/international/article/2017/03/14/l-estonie-premiere-cybervictime-de-moscou_5093948_3210.html

[4] Vitkine, 2017.

[5] Санжиев, 2007; Орлов, 2007.

хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[6].

Аналогичное определение также закреплено в Соглашении между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности[7], в Соглашении между Правительством Российской Федерации и Правительством Республики Беларусь[8] и в Соглашении между Правительством Российской Федерации и Правительством Китайской Народной Республики[9].

В Руководстве под киберпространством понимается среда, образованная физическими и нефизическими компонентами для хранения, модификации и обмена данными с использованием компьютерных сетей (Schmitt, 2013).

Также заслуживает внимания определение, разработанное совместной группой российских и американских специалистов. Они отметили, что под киберпространством понимается электронная среда, в которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается[10]. Данное определение, по сути, отражает саму суть киберпространства, но оно не учитывает одного важного момента. Речь идет о глобальном характере киберпространства, который обеспечивает возможность информационного обмена и взаимодействия, несмотря на государственные границы. Вместе с тем со стороны большинства государств наметилась тенденция установления суверенитета над своими национальными сегментами глобального киберпространства. Так называемый Закон о «суверенном Интернете»[11], принятый в России в 2019 г., иллюстрирует это.

Однако не следует отождествлять Интернет и киберпространство. Киберпространство включает в себя глобальную сеть Интернет, но не ограничивается ею. В подтверждение этого тезиса можно привести определение киберпространства, закрепленное в Доктрине информационной безопасности Российской Федерации, в которой данное понятие именуется информационной сферой. Здесь под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных

6 МИД России. (2011, сентябрь 22). *Конвенция об обеспечении международной информационной безопасности (концепция)*. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

7 Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Бюллетень международных договоров, Март 1993–2012, № 1, с. 13–21.

8 Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. Бюллетень международных договоров, Март 1993–2015, № 7, с. 16–23.

9 Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993–2016, № 11, с. 82–88.

10 Issuu. (2011, April 26). *The Russia — U. S. bilateral on cybersecurity: Critical terminology foundations*. https://issuu.com/ewipublications/docs/russia-us-terminology

11 Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Собрание законодательства Российской Федерации 2019, № 18, Статья 2214.

отношений[12]. Как видно из определения, Интернет не тождественен киберпространству. В доктрине также возможно найти подтверждение тезису о том, что не следует отождествлять Интернет и киберпространство (Danel'yan, 2020). Получается, киберпространство представляет собой совокупность компьютерных сетей, мобильных устройств и пользователей, которые взаимодействуют между собой на расстоянии, а Интернет является связующим каналом для такого взаимодействия.

С учетом вышеуказанного, считаем, что под киберпространством необходимо понимать глобальную электронную среду, образованную физическими и нефизическими компонентами, включая комплекс технических и программных средств, в которой посредством использования компьютерных и мобильных сетей, включая глобальную информационно-коммуникационную сеть «Интернет», осуществляется формирование, передача, прием, хранение, обработка, модификация и уничтожение информации.

Понятие вооруженного конфликта в киберпространстве

В Руководстве отдельной нормы-дефиниции вооруженного конфликта в киберпространстве не содержится, тем не менее такое определение содержится в пункте 2 комментария к норме 80. Под вооруженным конфликтом понимается ситуация, связанная с осуществлением военных действий, включая те, которые осуществляются с использованием киберсредств. Далее по тексту комментария, разработчики указали, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии, закрепленной в нормах 82 и 83 Руководства (Schmitt, 2013).

В норме 82 закреплено следующее: «Международный вооруженный конфликт имеет место всякий раз, когда между двумя или более государствами происходят военные действия, которые могут включать кибероперации или ограничиваться ими». В свою очередь, в норме 83 указано, что «немеждународный вооруженный конфликт возникает всякий раз, когда имеет место продолжительное вооруженное насилие, которое может включать или ограничиваться кибероперациями, происходящими между правительственными вооруженными силами и организованными вооруженными группами или между такими группами. Конфронтация должна достигать минимального уровня интенсивности, а вовлеченные в конфликт стороны должны обладать минимальной степенью организованности».

Как представляется, определение, закрепленное в комментарии к норме 80 Руководства, основано на нормах международного гуманитарного права и отражает суть вооруженного конфликта, но в то же время является достаточно общим. Ключевым моментом здесь является то, что такой конфликт осуществляется с использованием киберсредств, под которыми понимаются различные инструменты и методы, используемые в киберпространстве. На это указывают и в доктрине (Lin, 2012). Изучим их более подробно.

Для начала отметим, что предлагается две классификации таких инструментов и методов (Lin, 2012): во-первых, киберсредства можно разделить на автономные, способные работать без вмешательства человека, и на управляемые, которые работают под управлением оператора. Во-вторых, кибер-средства можно разделить на наступательные и оборонительные.

Очевидно, что первая классификация основана на техническом аспекте — в информационных технологиях, как известно, существуют автономные системы,

[12] Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента РФ от 5 декабря 2016 г. № 646. Собрание законодательства Российской Федерации 2016, № 50, Статья 7074.

которые работают без вмешательства человека, а также системы, управляемые оператором. В качестве критерия, лежащего в основе второй классификации, выступает военная тактика.

Предложенные классификации являются пересекающимися: автономные киберсредства могут быть как оборонительными, так и наступательными. Аналогично обстоит дело и с управляемыми киберсредствами. Рассмотрим автономные и управляемые средства, поскольку технический аспект является первичным.

Автономное наступательное киберсредство включает 3 необходимых элемента. Во-первых, доступ, под которым понимаются инструменты и методы, с помощью которых стороны конфликта получают информацию. Важно отметить, что в рамках киберпространства распространен удаленный доступ, который не требует близкого контакта между сторонами, что значительно отличает традиционный вооруженный конфликт от кибернетического.

Во-вторых, различные технические уязвимости той или иной информационной системы, которые позволяют ее взломать и получить доступ к интересующей информации. Сделать киберсистему полностью неуязвимой невозможно. Однако техническая уязвимость может быть оставлена в информационной системе намеренно и представлять собой «ловушку» для другой стороны кибернетического вооруженного конфликта.

И, наконец, в-третьих, так называемая полезная нагрузка, под которой понимается механизм воздействия на информационную систему после проникновения в нее в результате использования ее технической уязвимости. В качестве иллюстрации этого технического термина можно отметить, что, например, в случае компьютерного вируса полезной нагрузкой являются вредоносные действия такого программного обеспечения, которое и является примером автономного наступательного киберсредства. Компьютерные вирусы, как известно, действуют самостоятельно, и вполне возможно, что в ходе вооруженного конфликта в киберпространстве одна из воюющих сторон может использовать программное обеспечение, которое, взломав информационную систему противника, будет собирать необходимую информацию о противнике.

Что же касается автономных оборонительных киберсредств, то принцип их работы основан на использовании одного или нескольких вышеуказанных компонентов. Так, например, работа брандмауэра (файрвола) основана на принципе противодействия несанкционированному доступу в информационную систему, основанному на использовании технических уязвимостей системы.

Что же касается управляемых киберсредств, то тут все проще. Так как управляет таким инструментом оператор, т. е. человек, то объектом первичного воздействия будет именно он. Здесь применяются все те же традиционные наступательные методы по подкупу, вербовке и т. п. Оборонительными методами в таком случае будут различные мероприятия по предотвращению таких действий в отношении оператора.

Важно отметить, что данный подход не оспаривается в доктрине (Lin, 2012). В доктрине некоторые исследователи используют в отношении киберсредств термин «кибероружие» или «информационное оружие» (Talimonchik, 2015; Franklin, 2016; Hathaway et al., 2012; Pool, 2013). В то же самое время понятие «кибероружие» является более узким, поэтому более целесообразно использовать понятие «киберсредства».

Какие действия в киберпространстве могут осуществляться с использованием таких средств? Какие кибероперации существуют?

Так, большинство авторов классифицируют кибероперации на кибератаки и киберэксплуатацию (Lin, 2012; Schmitt, 2013).

В соответствии с нормой 92 Руководства, кибератака — это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей, либо к повреждению или разрушению объектов (Schmitt, 2013).

Определение кибератаки также содержится и в национально-правовых актах, например в ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ: «компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации»[13].

Данное определение, закрепленное в российском законе, является общим, и не учитывает специфику кибератак в условиях кибернетического вооруженного конфликта. Поэтому более целесообразным будет использование терминологии Руководства.

Киберэксплуатация, в свою очередь, — это кибероперации, направленные на проникновение в информационные системы противника с целью получения интересующей информации и не нарушающие их целостности и нормального функционирования. Как разумно отмечают в доктрине, лучшая киберэксплуатация — это та, которая незаметна для пользователей информационной системы, в которую осуществляется проникновение (Lin, 2012). Поэтому одним из примеров такой кибероперации является кибершпионаж. При этом в прессе порой отдельные кибероперации называют кибератаками, несмотря на то что такие кибероперации являются киберэксплуатацией.

Важно учитывать, что понятие «вооруженный конфликт» приобретает различное значение в зависимости от его типологии. Безусловно, международный вооруженный конфликт отличается от немеждународного в части их правового регулирования — это бесспорный факт. Тем не менее международный и немеждународный вооруженный конфликт являются частными случаями более общего понятия «вооруженный конфликт».

Итак, вооруженный конфликт в киберпространстве — это ситуация вооруженного столкновения и противостояния правительственных вооруженных сил двух и более государств, а также ситуация продолжительного вооруженного противостояния между правительственными вооруженными силами и организованными вооруженными группами или же между такими группами внутри одного государства, уровень напряженности насилия в которой превышает уровень напряженности в ситуациях нарушения внутреннего порядка и возникновения обстановки внутренней напряженности, в контексте которой сторонами такого противостояния используются киберсредства с целью осуществления различных кибероперациий в отношении друг против друга.

Отметим, что целесообразнее использовать понятие «кибернетический вооруженный конфликт», а не «кибервойна». Как известно, при разработке в далеком 1949 г. был использован термин «вооруженный конфликт», а не «война», т. к. первое понятие более широкое, чем второе. Надо полагать, что данная логика применима и к киберпространству. Несмотря на логичность такой аналогии, многие исследователи используют термин «кибервойна» (Zhang, 2012; Droege, 2012; Schmitt, 2002; Pool, 2013).

Теперь, определившись с основными понятиями, перейдем к предмету настоящей статьи.

[13] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Собрание законодательства Российской Федерации 2017, № 31, Статья 4736.

Ratione materiae МГП в киберпространстве

Для начала определимся с общим понятием военные действия или военные операции. Отправной точкой для этого является ст. 48 Дополнительного Протокола I, которая закрепила обычно-правовую норму, применяемую как в международных, так и немеждународных вооруженных конфликтах (Henckaerts & Doswald-Beck, 2006). В статье закреплено следующее: «Для обеспечения уважения и защиты гражданского населения и гражданских объектов стороны, находящейся в конфликте, должны всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими объектами и военными объектами и соответственно направлять свои действия только против военных объектов»[14].

Определяющим для военных действий (операций) является критерий направленности: они могут быть направленны только против военных целей, т. е. против комбатантов и военных объектов. Такой характер военных операций, в том числе и нападений, предопределен таким принципом международного гуманитарного права, как принцип проведения различия, который пронизывает все нормы, касающиеся вопросов ведения военных действий, как общего, так и конкретного характера. Так, в п. 1 ст. 51 Дополнительного Протокола I указано, что «гражданское население и отдельные гражданские лица пользуются общей защитой от опасностей, возникающих в связи с военными операциями»[15]. Пункт 2 данной статьи указывает, что «гражданское население как таковое, а также отдельные гражданские лица не должны являться объектом нападений»[16]; а в п. 3 закреплен запрет нападений неизбирательного характера[17].

В пп. «b» п. 5 ст. 51 Дополнительного Протокола I нашел отражение не только принцип проведения различия, но и принцип соразмерности: «В числе прочих следующие виды нападений следует считать неизбирательными: ...b) нападение, которое, как можно ожидать, попутно повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам, или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить»[18]. Этот принцип тесно связан с принципом проведения различия и, по сути, вытекает из него, на что указывают в доктрине (David, 2011).

Продолжая рассуждения о принципе проведения различия, отметим, что п. 6 ст. 51 Дополнительного Протокола I закрепил запрет нападений на гражданское население (отдельных гражданских лиц) в порядке репрессалий[19], а п. 2 ст. 52 закрепил, что нападения должны строго ограничиваться военными объектами[20].

И, наконец, п. 1 ст. 57 Дополнительного Протокола I закрепил вытекающий из принципа проведения различия принцип предосторожности: «При проведении военных операций постоянно проявляется забота о том, чтобы щадить гражданское население, гражданских лиц и гражданские объекты»[21].

---

[14] Дополнительный протокол (Протокол I) к Женевским конвенциям касающийся защиты жертв международных вооруженных конфликтов ст. 48, Август, 12, 1949, с. 264. [далее — Женевский протокол (I)].

[15] Женевский протокол (I), 265.

[16] Женевский протокол (I), 265.

[17] Женевский протокол (I), 265.

[18] Женевский протокол (I), 265.

[19] Женевский протокол (I), 266.

[20] Женевский протокол (I), 266.

[21] Женевский протокол (I), 269.

Отметим также, что еще одним ограничивающим военные действия фактором является принцип гуманности, который аналогично является одним из ключевых принципов международного гуманитарного права, что прослеживается в нормах этой отрасли международного права, включая выше проанализированные нормы.

Таким образом, все военные действия ограничены вышеуказанными принципами гуманности, проведения различия, соразмерности и предосторожности. Установив этот очевидный факт, перейдем теперь к поставленному выше вопросу в отношении кибероперациий.

В отношении данного вопроса в доктрине существует 3 точки зрения. Первая является наиболее поддерживаемой: большинство исследователей придерживаются мнения, что несмотря на то, что содержание норм Дополнительного Протокола I, в частности его ст. 48 и следующих за ней статей, свидетельствуют о верховенстве в международном гуманитарном праве принципа защиты гражданского населения, только те кибероперации, которые являются нападением (кибератаками), попадают под действие вышеуказанных принципов МГП, в частности, под действие принципа проведения различия (Schmitt, 2011; Geiß & Lahmann, 2012). Так, M. N. Schmitt (2011) выдвигает аргумент, согласно которому определенные военные операции могут быть специально направлены против гражданского населения, в частности, психологические операции, следовательно, не все военные действия в киберпространстве будут ограничиваться принципом проведения различия.

Другая позиция была высказана N. Melzer (2011): научные споры в отношении понятия «нападение» не дают достаточно удовлетворительного ответа на данный вопрос, поскольку нормы права, регулирующие ведение военных действий, применяются ко всем военным операциям, а не только к нападениям. В частности, ученый указывает, что применение закрепленных нормами международного гуманитарного права по отношению к военным операциям ограничений к кибероперациям зависит не от квалификации такой кибероперации в качестве нападения, а от того, является ли такая кибероперация частью военных действий, как это подразумевается в МГП. Исходя из этого, он приходит к выводу о том, что кибероперации должны признаваться военными действиями в случаях, если они направлены на причинение ущерба противной стороне, на причинение смерти или увечий людям, а также на разрушение и повреждение различных объектов, либо в ситуациях, когда они имеют своей целью негативное влияние на военный потенциал противника. Следовательно, в качестве примера кибероперациий, являющихся военными действиями, можно привести такие операции, которые направлены на нарушение функционирования информационных инфраструктур и сетей, с помощью которых противник управляет системам различных вооружений, при этом не требуется, чтобы таким сетям и инфраструктурам был причинен физический вред.

Если взять за основу подход N. Melzer (2011), то из-под понятия «военные действия» выпадают кибероперации, направленные на сбор разведывательных данных. Как известно, разведка также является формой военных действий, поэтому данный подход не отражает ту концепцию военных действий, которая отражена в нормах права вооруженных конфликтов.

Что касается утверждения о том, что не требуется причинения физического ущерба, то N. Melzer (2011) все-таки не делает конкретного вывода, ограничиваясь указанием на проблему нахождения баланса между ограничительным и разрешительным толкованием права.

Принимая во внимание цели норм МГП, в соответствии с которыми «мирное гражданское население должно оставаться за пределами военных действий, насколько это возможно,

и пользоваться общей защитой от опасности, вытекающей из военных действий» (Sandoz et al., 1987), позицию N. Melzer (2011) можно охарактеризовать как верную. Тем не менее в таком случае останется открытым вопрос о том, являются ли операции, направленные на нарушение функционирования гражданской инфраструктуры, военными действиями.

Третья точка зрения была высказана H. H. Dinniss (2012), согласно которой запрет нападений на гражданское население и гражданские объекты распространяется не только на нападения, как таковые. Основываясь на содержании ст. 48, 51 и 57 Дополнительного Протокола I, ученый указывает, что гражданские лица пользуются защитой от военных операций в целом, включая нападения; и поэтому принципы МГП полностью применимы к кибероперациям, в том числе и к кибератакам, которые являются военными действиями, при этом кибератаки должны соотноситься с применением традиционной вооруженной силы, но необязательно должно приводить к таким же последствиям.

Критикуя позицию H. H. Dinniss (2011), C. Droege (2012) отмечает, что в нормах МГП содержится дихотомия между военными операциями и нападениями, чего не учитывает подход Г.Г. Харрисон.

Указанная дихотомия ни в коем случае не влияет на применение к нападениям принципов МГП — ведь определение нападения закрепили лишь потому, что оно является одной из основных военных операций, т. е. является частным явлением общего понятия «военные операции». Кроме того, позиция H. H. Dinniss (2012) лишний раз подтверждает факт, что принципы МГП применяются ко всему комплексу военных действий.

Вернемся к первой точке зрения, выдвинутой M. N. Schmitt (2011), согласно которой психологические операции входят в понятие «военные действия». Отметим, что в доктрине обосновано звучат голоса, что эта позиция основана на неверном толковании концепции военных действий (Droege, 2012). Напомним, что, как справедливо указывают в доктрине (David, 2011), моральный дух врага не является военной целью. Следовательно, действия, направленные на подрыв морального духа врага, в том числе, направленные против его гражданского населения, никак не могут являться военными операциями.

Видимо, M. N. Schmitt (2011) основывал свои рассуждения на тезисе У. Черчилля о том, что «моральный дух неприятеля — тоже военный объект». Мы же обратимся к юридической стороне вопроса о понятии военных операций. Как отмечают в Комментарии к ст. 48 Дополнительного Протокола I, понятие «военные действия» относится ко «всем передвижениям и актам, связанным с военными действиями, которые осуществляются вооруженными силами» (Sandoz et al., 1987). В комментарии к ст. 51 под военными операциями понимаются «все передвижения и деятельность, осуществляемые вооруженными силами в связи с военными действиями» (Sandoz et al., 1987). И, наконец, в комментарии к ст. 57 под военными действиями понимаются «любые передвижения, маневры и любая другая деятельность, осуществляемые вооруженными силами в отношении боевой цели» (Sandoz et al., 1987).

Таким образом, психологические операции, пропаганда, а также шпионаж не относятся к понятию «военные действия». Также отметим, что целью принципов МГП является ограничение всего спектра военных операций, включая нападения. Поэтому надо полагать, что применительно к киберпространству под ограничения, налагаемые МГП, попадают все кибероперации, которые могут быть приравнены к военным действиям в целом, а не только к кибератакам. Это и есть *ratione materiae* международного гуманитарного права в киберпространстве. Аналогичной точки зрения придерживаются и разработчики Руководства.

Ratione temporis МГП в киберпространстве

Исходя из общей ст. 2 Женевских конвенций[22], нормы МГП к киберпространству применяются либо с момента начала вооруженного конфликта, в котором совершаются кибероперации, либо с момента начала вооруженного конфликта, ограниченного киберпространством, без применения традиционной вооруженной силы. Эта составляющая вопроса о *ratione temporis* не вызывает каких-либо трудностей. Сложности возникают при ответе на вопрос об окончании применения таких норм к киберпространству.

Как установлено ст. 6 Женевской конвенции IV[23] и п. «b» ст. 3 Дополнительного Протокола I[24], нормы права вооруженных конфликтов прекращают свое действие по окончанию военных действий. В Комментарии МККК указано, что под окончанием военных действий понимается, в том числе, «последний залп» (Pictet, 1958), заключение перемирия, капитуляция и т. п. (Pictet, 1958; Sandoz et al., 1987). Применительно к киберпространству, моментом окончания следует считать момент завершения последней кибероперации, совершенной в контексте классического или кибернетического вооруженного конфликта. Однако данный вывод все-таки является исключительно теоретическим, поскольку отсутствует соответствующая практика государств.

Вопросы также возникают в отношении окончания оккупации, плена и интернирования. Уже упомянутый пункт «b» ст. 3 Дополнительного Протокола I устанавливает, что МГП прекращает применяться в момент окончания оккупации[25]; ст. 5 Женевской Конвенции III связывает окончание применения норм МГП с моментом окончания плена (полное освобождение военнопленных и их репатриация)[26], а ст. 6 Женевской конвенции IV указывает в этом плане на момент окончания интернирования[27]. Надо полагать, что ко всем кибероперациям, совершенным до обозначенных моментов, будут применяться нормы МГП. Тем не менее данный вывод снова остается исключительно теоретическим.

Проблема квалификации кибератаки в рамках вооруженного конфликта

Кибератаки отличаются от традиционных нападений тем, что не предполагают классического применения вооруженной силы (применение насилия). П. 1 ст. 49 Дополнительного Протокола I устанавливает, что под нападениями понимаются акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне[28]. Выходит, применение насилия не указывает на средства нападения. Под средствами нападений принято понимать средства, имеющие кинетический эффект (Dinstein, 2016; Schmitt, 2011; Franklin, 2018). Военные действия, в ходе которых применяется оружие, приводящие к серьезным разрушениям и повреждениям объектов и к причинению смерти и увечий, являются нападениями, даже в случае, если отсутствует применение физической силы. Такой вывод

[22] Женевский протокол (I), 240.

[23] Женевская конвенция о защите гражданского населения во время войны, ст. 6, Август, 12, 1949, с. 171. [далее — Четвертая женевская конвенция].

[24] Женевский протокол (I), 241.

[25] Женевский протокол (I), 241.

[26] Дополнительный протокол (Протокол III) к Женевским конвенциям касающийся принятия дополнительной отличительной эмблемы ст. 5, Август, 12, 1949, с. 241. [далее — Женевский протокол (III)].

[27] Четвертая женевская конвенция, 84.

[28] Женевский протокол (I), 264.

подтверждается практикой[29]. Поэтому достаточно долгое время считалось, что определяющим фактором для квалификации военной операции в качестве нападения является не насильственный характер используемых в ее ходе средств, а серьёзность последствий такой операции (Schmitt, 2002; Schmitt, 2013). Признать кибератаки нападениями по смыслу МГП достаточно сложно.

В этом контексте научные споры идут в отношении кибератак, которые не приводят к разрушениям и повреждениям объектов, к смертям и ранениям людей, но приводят к нарушению нормального функционирования атакуемых объектов без какого-либо физического повреждения или разрушения. Негативное влияние таких кибератак в физическом пространстве может быть минимальным с точки зрения того уровня насилия, которое требуется для квалификации деяния в качестве нападения: например, будет прекращена подача электроэнергии или подача питьевой воды, либо будет нарушена система банковских онлайн-платежей и т. п. Возникает закономерный вопрос: могут ли такие кибератаки квалифицироваться в качестве нападения по смыслу ст. 49 Дополнительного Протокола I?

В доктрине можно выделить две основных точки зрения на эту проблему. Первая была выдвинута M. N. Schmitt (2002; 2011). Однако следует учитывать, что его позиция претерпела некоторую эволюцию. В ранних работах ученый отмечал, что кибератака является нападением в соответствии со ст. 49 Дополнительного Протокола I, если она причиняет смерть или увечья людям, вне зависимости от того, являются ли они комбатантами или гражданскими лицами, либо приводит к повреждениям или разрушению объектов как военных, так и гражданских. Таким образом, для признания кибератаки нападением необходимо наличие указанных серьезных последствий в физическом мире. Что касается кибератак, которые причиняют лишь временные неудобства или нарушают нормальное функционирование атакуемой информационной системы, нападением по смыслу ст. 49 Дополнительного Протокола I они не являются.

Несколько позже указанный автор изменил свой подход. И теперь под уничтожением, к которому должна приводить кибератака для того, чтобы ее можно было квалифицировать в качестве нападения, также понимает последствия, которые хоть и не причиняют физического уничтожения (повреждения), но «ломают» информационную систему, выводят ее из строя, что делает невозможным нормальное ее функционирование (Schmitt, 2012a; Schmitt, 2012b; Schmitt, 2014; Schmitt, 2019).

Альтернативная точка зрения была выдвинута К. Дёрманом. Так, по мнению ученого, кибератаки могут являться нападением, даже если отсутствуют традиционные последствия нападений в физическом мире[30]. Такой подход, по сути, основан на п. 2 ст. 52 Дополнительного Протокола I, согласно которому одним из способов воздействия на военные объекты, наряду с разрушением (полное и частичное) и захватом, является нейтрализация[31]. Как отмечает К. Дёрман, нейтрализация вовсе не означает был ли выведен атакуемый военный объект из строя посредством разрушения, уничтожения или посредством любого другого способа[32].

Его оппонент, М.Н. Шмитт, поначалу выразил несогласие с предложенной теорией нейтрализации, указав, что ст. 52 Дополнительного Протокола I, определяющая военные объекты,

---

29 Prosecutor v. Tadić, Case No. IT-94-1-T, decision on the defence motion for interlocutory appeal on jurisdiction. 120, 124 (Int'l Crim. Trib. For the Former Yugoslavia Oct. 2, 1995).

30 Dörmann, K. (2004). *Applicability of the additional protocols to computer network attacks*. ICRC. https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf

31 Женевский протокол (I), 54.

32 Dörmann, 2004.

не имеет отношения к делу, поскольку сама сущность военного объекта предполагает нападение, но не определяет его (Schmitt, 2011). Тем не менее после эволюции его взглядов он принял теорию, предложенную К. Дёрманом, (Schmitt, 2014).

Понять первичную критику позиции K. Dörmann со стороны M. N. Schmitt можно. Она основана на теории, сторонники которой отрицали то, что нейтрализация может предполагать нападение на военный объект не с целью его разрушения или повреждения, а с целью недопущения его использования противной стороной (Bothe et al., 1982). Надо полагать, что эта теория не отвечает реальному положению дел. Многие боевые задачи достаточно часто заключаются в том, чтобы ограничить противнику доступ к какому-либо военному объекту. Особенно это касается вооруженного конфликта в киберпространстве. Достаточно помыслить следующую возможную ситуацию: система противоракетной обороны противной стороны может быть нейтрализована на определенное время вследствие кибератаки, которая нарушит ее функционирование, но не причинит какого-либо вреда ее физической инфраструктуре. В доктрине большинство исследователей поддерживают теорию, выдвинутую K. Dörmann (Droege, 2012; Pool, 2013; Kelsey, 2008; Hathaway et al., 2012).

Обратимся теперь к Руководству. В норме 92 закреплено следующее определение кибератаки: «кибератака — это наступательная или оборонительная кибероперация, которая, как разумно ожидается, приведет к причинению травм или смерти людей, либо к повреждению или разрушению объектов» (Schmitt, 2013).

Очевидным фактом является то, что данная норма Руководства отражает точку зрения M. N. Schmitt, что не удивительно, т. к. он является редактором Руководства. Более того, в п. 2 комментария к данной норме прямо указано, что основой для нее послужил п. 1 ст. 49 Дополнительного Протокола I (Schmitt, 2013). Однако пп. 10–13 свидетельствуют о том, что разработчики Руководства не пришли к единому мнению относительно содержания понятия «повреждение объектов», в частности, входит ли в это понятие нарушение функционирования объекта (Schmitt, 2013).

В связи с этим необходимо согласиться с C. Droege (2012), которая указывает на ограничительный характер теории, предложенной М.Н. Шмиттом. Действительно, абсурдным представляется вывод, согласно которому объект, выведенный из строя кибератакой, не является поврежденным. Иными словами, будет ли разница в последствиях для гражданского населения в случае разрушения сети энергоснабжения в результате бомбардировки и в ситуации выведения этой сети из строя посредством кибератаки? По нашему мнению, последствия будут идентичными, и поэтому можно прийти к выводу, что критерий наличия физического повреждения, не является идеальным.

Разумной также выглядит ссылка C. Droege (2012) на принцип соразмерности, который предполагает наличие сопутствующего ущерба, но также предполагает защиту гражданских объектов и гражданского населения от случайного ущерба. Очевидно, что понятие «ущерб» отличается по содержанию от понятия «уничтожение». Под ущербом в указанном контексте необходимо понимать причиненный вред, в результате которого поврежденный объект теряет какие-либо свои полезные свойства. Поэтому вполне логично считать ущербом нарушение нормального функционирования различных инфраструктур в результате кибератак.

В то же самое время необходимо понимать, что нарушение нормального функционирования в киберпространстве — это явление временного характера, поскольку поврежденная система и данные в ней всегда могут быть восстановлены. По этой причине логично квалифицировать

кибератаки в качестве нападения даже в том случае, когда они привели к временному нарушению нормального функционирования инфраструктуры без ее физического разрушения или повреждения.

Вышеуказанные замечания позволяют говорить о расширительном толковании понятия «нападение» применительно к киберпространству. Тем не менее, если взять за основу расширительный подход, то можно прийти к абсурдному выводу, что все кибератаки, направленные против гражданских информационных систем, необходимо признавать нападениями по смыслу МГП. В таком случае напрочь стирается граница между кибернетическим уголовным правом и МГП. В связи с этим надо согласиться с C. Droege (2012), высказавшей опасение, что «приравнивание к нападениям таких нарушений ... выходит за границы предполагаемой сферы действия норм ведения военных действий».

M. N. Schmitt (2002; 2011), в свою очередь, в качестве критерия, позволяющего отграничить кибератаки, являющиеся нападениями по смыслу МГП, от актов киберпреступности, предлагает критерий неудобства. Но что считать неудобством? Представляется, что данный критерий является достаточно расплывчатым.

Надо полагать, что для разрешения этой проблемы поможет концепция «критической инфраструктуры», предложенная N. Melzer (2011). Более того, данный подход уже отражен в существующих договорах по информационной безопасности и некоторых национальных правовых актах (в частности, в российских)[33]. Так, в соответствующем Соглашении между Правительством Российской Федерации и Правительством Китайской Народной Республики понятие «объекты критической информационной инфраструктуры» определено наиболее полным образом: «Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети государственных органов; информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, предназначенные для обеспечения обороны страны, безопасности государства и правопорядка, а также функционирующие в области здравоохранения, транспорта, связи, в кредитно-финансовой сфере, в оборонно-промышленном и топливно-энергетическом комплексах, в атомной, ракетно-космической и химической промышленности, в отраслях промышленности с непрерывным циклом производства»[34]. Выходит, что кибератака, нарушающая нормальное функционирование именно таких объектов (без их физического разрушения), должна считаться нападением по смыслу МГП. Тем не менее при всей очевидности вывода здесь также необходима соответствующая практика государств.

[33] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Бюллетень международных договоров, Март 1993–2012, № 1, с. 13–21; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. Бюллетень международных договоров, Март 1993–2015, № 7, с. 16–23; Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993–2016, № 11, с. 82–88; Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Собрание законодательства Российской Федерации 2017, № 31, Статья 4736.

[34] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. Бюллетень международных договоров, Март 1993-2016, № 11, с. 82–88.

Выводы и дискуссия

В результате проведенного исследования, было выявленно:

1. Под ограничения военных действий, установленные нормами МГП, попадают все кибероперации, которые приравниваются к таким военным действиям (*ratione materiae*).

2. Что касается вопроса о действии во времени норм МГП в киберпространстве (*ratione temporis*), то началом применения норм необходимо считать момент возникновения вооруженного конфликта, в рамках которого совершаются кибероперации, либо момент возникновения вооруженного конфликта, ограниченного киберпространством, без применения традиционной вооруженной силы. Напротив, проблема окончания применения таких норм остается в известной степени теоретической, поскольку отсутствует соответствующая практика государств.

3. Кибератака будет квалифицироваться как нападение по смыслу МГП в случаях, если она приводит к гибели людей, причинению им увечий, физическому разрушению или повреждению объектов, а также в ситуациях, когда нарушается нормальное функционирование объектов критической информационной инфраструктуры без физического их разрушения или повреждения.

Не последнюю роль в вопросах *ratione materiae* и *ratione temporis* МГП в киберпространстве, а также в вопросе квалификации кибератаки в качестве нападения по смыслу МГП играет практика государств. Более того, практика государств играет большую роль для развития соответствующих норм международного права в отношении киберпространства в целом, поэтому ее необходимо развивать.

Первой мыслью по решению вышеуказанной проблемы практики, которая приходит на ум, является предложение о разработке соответствующего международного договора. Однако, во-первых, процесс создания международного договора, как известно, достаточно продолжителен по времени. Есть вероятность, что разработка такого международного договора может занять даже не годы, а десятилетия.

Во-вторых, на сегодняшний день очевидно, что не все государства поддерживают инициативу разработки и принятия такого международного договора, достаточно вспомнить российский проект Конвенции о международной информационной безопасности, не имевший успеха при рассмотрении в ООН. Поэтому, на наш взгляд, на данный момент самым приемлемым решением остается развитие соответствующей практики государств.

Заключение

Итак, ключевым является вывод о необходимости разработки практики государств по вопросам предметных и временных рамок применения норм международного гуманитарного права в киберпространстве, а также по вопросу правовой квалификации кибератаки. Тем не менее помимо этого очевидного вывода, представляется правильным не только ждать момента, когда соответствующая практика будет сформирована, но также, чтобы международное сообщество использовало другие способы для решения данной проблемы. В частности, необходимо вынесение этой проблемы на рассмотрение в пленарные органы международных организаций, например, в Генеральную Ассамблею Организации Объединенных Наций. По нашему мнению, целью создания такой практики и международного договора является не разработка новых норм международного гуманитарного права, которые заменят существующие, а адаптация существующих норм применительно к киберпространству.

Список литературы / References:

1. Backstrom, A. & Henderson, I. (2012). New capabilities in warfare: An overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, *94*(886), 483–514.
2. Bothe, M., Partsch, K. J. & Solf, W. A. (1982). *New rules for victims of armed conflicts: Commentary to the two 1977 protocols additional to the Geneva Conventions of 1949*. Martinus Nijhoff Publishers.
3. Brown, G. D. (2011). Why Iran didn't admit Stuxnet was an attack. *Joint Force Quarterly*, *63*, 70–73.
4. Buchan, R. (2012). Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law*, *17*(2), 211–227.
5. Danel'yan, A. A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstava [International legal regulation of cyberspace]. *Obrazovanie i Pravo*, *1*, 261–269.
6. David, E. (2011). *Printsipy prava vooruzhennykh konfliktov: Kurs lektsii, prochitannykh na yuridicheskom fakultete Otkrytogo Brussel'ckogo Universiteta* [Principes de droit des conflits armés: Précis de la faculté de droit de l'Université Libre de Bruxelles]. CICR.
7. Dinniss, H. H. (2012). *Cyber warfare and the laws of war*. Cambridge University Press.
8. Dinstein, Y. (2016). *The conduct of hostilities under the law of international armed conflict* (3rd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781316389591
9. Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533–578.
10. Franklin, A. (2018). An international cyber warfare treaty: Historical analogies and future prospects. *Journal of Law & Cyber Warfare*, *7*(1), 149–164.
11. Geiß, R. & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. *Israel Law Review*, *45*(3), 381–399. https://doi.org/10.1017/S0021223712000179
12. Hathaway, O. A., Crootof, R., Levitz, Ph., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817–885.
13. Henckaerts, J.-M. & Doswald-Beck, L. (2006). *International Commitee of the Red Cross. Customary international humanitarian law. Volume I: Rules*. Cambridge University Press.
14. Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 106*(7), 1427–1451. https://repository.law.umich.edu/mlr/vol106/iss7/6
15. Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515–531.
16. Melzer, N. (2017). *International humanitarian law: A comprehensive introduction*. International Commitee of the Red Cross.
17. Melzer, N. (2011). *Cyberwarfare and international law*. The United Nations Institute for Disarmament Research (UNIDIR).
18. Demeyere, B., Henckaerts, J.-M., Hiemstra, H., & Nohle, E. (2016). The updated ICRC commentary on the Second Geneva Convention: Demystifying the law of armed conflict at sea. *International Review of the Red Cross*, *98*(2), 401–417. https://doi.org/10.1017/S1816383117000376
19. Pool, P. (2013). War of the cyber world: The law of cyber warfare. *The International Lawyer*, *47*(2), 299–323.
20. Sandoz, Y., Swinarski, C. & Zimmermann, B. (Eds.). (1987). *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. International Commitee of the Red Cross, Kluwer Academic Publishers.

21. Schmitt, M. N. (2019). Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, *101*(1), 333–355.
22. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
23. Schmitt, M. N. (2014). Rewired warfare: Rethinking the law of cyber attack. *International Review of the Red Cross*, *96*(893), 189–206.
24. Schmitt, M. N. (Eds.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
25. Schmitt, M. N. (2012a). "Attack" as a term of art in international law: The cyber operations context. *4th International Conference on Cyber Conflict Proceedings* (pp. 283–293). Tallinn.
26. Schmitt, M. N. (2012b). Classification of cyber conflict. *Journal of Conflict and Security Law*, *17*(2), 245–260. https://doi.org/10.1093/jcsl/krs018
27. Schmitt, M. N. (2011). Cyber operations and the jus in bello: Key issues. *Naval War College International Law Studies*, *87*, 89–110. https://digital-commons.usnwc.edu/ils/vol87/iss1/7/
28. Schmitt, M. N. (2010). Cyber operations in international law: The use of force, collective security, self-defense and armed conflict. *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 151–178). National Research Council, Washington D. C.
29. Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365–399.
30. Talimonchik, V. P. (2015). International legal means of combating information weapons. *Russian Yearbook of International Law*, Special Issue, 135–151.
31. Tikk, E., Kaska, K. & Vihul, L. (2010). *International cyber incidents: Legal considerations*. CCDCE.
32. Zhang, L. (2012). A Chinese perspective on cyber war. *International Review of the Red Cross*, *94*(886), 801–807.

Сведения об авторе:

Гаркуша-Божко С. Ю. — магистр международного права, юрисконсульт Школы высшего спортивного мастерства по водным видам спорта имени Ю. С. Тюкалова, Санкт-Петербург, Россия.
garkusha-bozhko.sergej@yandex.ru
ORCID 0000-0003-1253-3157

Information about the author:

Sergey Y. Garkusha-Bozhko — LLM in Law, Legal Advisor, School of Higher Sportsmanship in Water Sports named after Yu. S. Tyukalov, St. Petersburg, Russia.
garkusha-bozhko.sergej@yandex.ru
ORCID 0000-0003-1253-3157

https://doi.org/10.38044/2686-9136-2021-2-1-83-93

СТАТЬИ

ЦИФРОВИЗАЦИЯ ГОСКОМПАНИЙ

А.В. Савоськин*, Н.А. Рожкова

Уральский государственный экономический университет,
620144, Россия, Екатеринбург, ул. 8 Марта, 62

Аннотация

В статье анализируются правовые акты, регулирующие общественные отношения в сфере цифровой трансформации государственных корпораций и компаний с государственным участием. При этом целью исследования является установление приоритетных организационно-экономических и управленческих направлений такого реформирования и их проектируемое содержание. Достижение целей исследования обеспечивается использованием формально-юридических методов познания. Прежде всего, статья обращает внимание на выработку целей цифровой трансформации госкомпании исследуя такие трансформации как: создание целевой бизнес-модели, системы целей и ключевых показателей эффективности цифровой трансформации, определение стратегических направлений развития цифровой трансформации и горизонтов планирования стратегии цифровой трансформации. При этом отдельное внимание уделяется разработке и реализации инициатив по внедрению цифровых решений и цифровой инфраструктуры; развитию поставщиков цифровых решений; организационным мероприятиям в рамках цифровой трансформации; мероприятиям по программному импортозамещению; а также мероприятиям по обеспечению информационной безопасности в рамках цифровой трансформации. Самостоятельным направлением цифровой трансформации госкомпаний признано совершенствование «качества» их кадрового состава и формирование культуры цифровой трансформации. Это потребовало обособление таких направлений как: выработка модели цифровых компетенций и кадрового обеспечения цифровой трансформации госкомпании; оценка потребности в кадрах, обладающих специальной компетенцией; обучение цифровым навыкам и развитие цифровых компетенций сотрудников госкомпании; управление сотрудниками цифровых специальностей; планирование и проведение мероприятий по развитию цифровой культуры и культуры информационной безопасности госкомпании. В завершении делается вывод об универсальности предлагаемых направлений цифровизации госкомпаний и их применимости к деятельности иных организаций (прежде всего частных).

Ключевые слова

цифровизация, цифровая трансформация, государственная компания, государственная корпорация, дорожная карта, цифровая инфраструктура, цифровая безопасность

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Савоськин, А. В., Рожкова, Н. А. (2021). Цифровизация госкомпаний. *Цифровое право, 2*(1), 83–93. https://doi.org/10.38044/2686-9136-2021-2-1-83-93

* Автор, ответственный за переписку

Поступила: 04.12.2020; принята в печать: 09.03.2021; опубликована: 31.03.2021

ARTICLES

DIGITALIZATION OF STATE COMPANIES

Alexander V. Savoskin*, Natalia A. Rozhkova

Ural State Economic University,
62, str. March 8, Yekaterinburg, Russia, 620144

Abstract

The article analyzes the legal acts that regulate public relations regarding the digital transformation of state corporations and companies with state participation. The economic and managerial directions of reform of the highest priority are established. The article describes the goals of the digital transformation of a state-owned company, including: creating a target business model, a system of goals and key performance indicators of digital transformation, and determining a digital transformation strategy. Special attention is paid to the development and implementation of initiatives for the implementation of digital infrastructure; the development of digital solutions providers; organizational activities within the framework of digital transformation; measures for programmed import substitution; and measures to ensure information security within the framework of digital transformation. Considering independent directions the digital transformation of state-owned companies can take, one such is the improvement of the "quality" of the staff and the formation of a culture of digital transformation. The article highlights such areas of work as: the creation of a model of digital competencies and the staffing of digital transformation within a state company; an assessment of the need for employees with special competence; teaching digital skills; the development of employees' digital competencies within a state company; digital workforce management; and planning and holding an event to develop digital culture and the information security culture of a state company. In conclusion, it is determined that the proposed areas of the digitalization of state-owned companies are universal. It is suggested that these recommendations be used in relation to other organizations (primarily private).

Keywords

digitalization, digital transformation, state-owned company, state-owned corporation, road map, digital infrastructure, digital security

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Savoskin, A. V., & Rozhkova, N. A. (2021). Digitalisation of state companies. *Digital Law Journal, 2*(1), 83–93. https://doi.org/10.38044/2686-9136-2021-2-1-83-93

* Corresponding author

Submitted: 4 Dec. 2020, accepted: 09 Mar. 2021, published: 31 Mar. 2021

Введение

Президентом РФ в Указе от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» поставлена задача к 2030 году «обеспечить цифровую трансформацию». Новая национальная цель развития России пришла на смену ранее установленной цели «обеспечения ускоренного внедрения цифровых технологий в экономике и социальной сфере» (Указ Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»). Не трудно заметить, что в настоящее время задача поставлена более чем широко. Вместе с тем по справедливому замечанию Williams et al. (2018), именно в цифровизации экономических отношений наблюдается наибольший прогресс (что в целом вполне закономерно, так как изначально акцент был сделан на эту сферу).

Безусловно, решение грандиозной задачи, поставленной главой государства, потребует больших усилий в самых разных сферах жизни (Karasev et al., 2019). Не ставя перед собой цели определения и раскрытия всех направлений цифровой трансформации в России, хотелось бы обратить внимание на перспективы цифровизации государственных корпораций и компаний с государственным участием (далее госкомпании). Такие субъекты гражданских отношений наиболее подвержены нормативному воздействию государства (как своего учредителя) и как раз они являются примером цифровизации для иных организаций (прежде всего частных). Кроме того именно госкомпании зачастую создают необходимую инфраструктуру цифровизации (Álvarez Royo-Villanova, 2020). Например, пилотный проект Сбербанка РФ, с 2018 года осуществляющий сбор биометрических данных. Более того, госкомпании могут использовать целевое государственное финансирование для внедрения новых электронных технологий и средств в организацию своей деятельности.

Вместе с тем перед госкомпаниями в России стоит нетривиальный вопрос, что означает «цифровая трансформация» и в чем она должна выражаться? Сложность ответа на этот вопрос заключается в двух обстоятельствах. Во-первых, в РФ отсутствует комплексный федеральный закон, который бы определял направления цифровой трансформации, ее этапы, ответственных лиц, источники финансирования или хотя бы легализовал используемый понятийный аппарат. Во-вторых, сегодня вопросы цифровизации регулируются крайне большим числом разрозненных актов, многие из которых вообще не входят в традиционную для России систему источников права. Например, значительный массив положений содержит национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. Вместе с тем сам Совет при Президенте Российской Федерации по стратегическому развитию и национальным проектам не является органом власти и юридическая сила его решений неясна (что, кстати, подтверждается и формой акта — протокол).

Таким образом, целями настоящей публикации является уяснение правого поля цифровой трансформации, то есть тех актов, которые что-либо определяют в сфере цифровизации (прежде всего госкомпаний), а также направлений цифровизации госкомпаний. Думается, что в современных условиях такой перечень сам по себе обладает ценностью.

Мы предлагаем включить следующие акты:

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационного общества Российской Федерации на 2017–2030 годы» и принятые в его развитие перечни поручений Президента Российской Федерации от 24 января 2020 г. № Пр-113 и от 3 июля 2020 г. № Пр-1068.

2. Национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

3. Паспорт федерального проекта «Цифровые технологии», утвержденный протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

4. Паспорт федерального проекта «Информационная безопасность», утвержденный протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

5. Паспорт федерального проекта «Кадры для цифровой экономики», утвержденный протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

6. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”».

7. Постановление Правительства Российской Федерации от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации».

8. Постановление Правительства Российской Федерации от 10 июля 2019 г. № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации».

9. Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» и другие.

Главным недостатком законодательного регулирования является пробел именно в законодательном, а не подзаконном правовом регулировании, поскольку специальный акт высшего уровня о цифровой трансформации в России не принят на настоящий момент. Еще одной проблемой является фрагментарность правового регулирования цифровизации.

Вместе с тем анализ приведенных выше актов (и некоторых других) позволяет выделить следующие направления цифровой трансформации государственных корпораций и компаний с государственным участием:

1. Анализ текущего состояния и перспективы цифровой трансформации госкомпании.
2. Выработка целей цифровой трансформации госкомпании.
3. Разработка дорожной карты цифровой трансформации госкомпании.
4. Совершенствование «качества» кадрового состава госкомпании и формирование культуры цифровой трансформации.

Безусловно, предлагаемый подход является обобщенным и примерным, но он позволит комплексно представить ответ на вопрос, что конкретно необходимо сделать, и в известной мере ответить на вопрос — в каком порядке проводить изменения. Далее, используя формально-юридический правовой метод исследования, проанализируем каждое направление отдельно.

Анализ текущего состояния госкомпаний и перспектив их цифровой трансформации

Это направление цифровой трансформации предполагает проведение аналитики цифровой трансформации отрасли, оценку цифровой зрелости госкомпании, исследование ключевых вызовов и возможностей для цифровой трансформации, а также рисков и угроз информационной безопасности в ходе реализации цифровой трансформации, в различных, в том числе чрезвычайных условиях (Frolov & Bosenko, 2020).

При этом сложность анализа заключается в том, что государственная корпорация, с одной стороны, реализует поставленные перед ней социально-экономические значимые для общества цели, но с другой, действует и как хозяйствующий субъект — осуществляет предпринимательскую деятельность, получает прибыль, инвестирует средства.

Отметим, что анализ цифровой трансформации отрасли предполагает исследование:

- изменений в поведении потребителей;
- изменений в бизнес-моделях игроков отрасли;
- появление новых онлайн-платформ и цифровых экосистем;
- изменений в технологических векторах цифровой трансформации;
- изменений в качестве внешних условий для цифровой трансформации (например, условия финансирования, меры государственной поддержки, образовательные программы).

Оценка цифровой зрелости предусматривает анализ ключевых направлений цифровой трансформации и ключевых элементов базовых корпоративных условий для цифровой трансформации. Оценка цифровой зрелости также включает текущий уровень использования современных цифровых технологий и программного обеспечения для цифровой трансформации, а также новейших достижений в области передачи данных (Tadayoni et al., 2018).

Определение ключевых вызовов и возможностей, созданных цифровой трансформацией для повышения конкурентоспособности и развития госкомпании крайне желательно. Ключевые вызовы и возможности учитывают изменения, которые происходят в отрасли за счет цифровой трансформации и влияют на позиции госкомпании на рынке. Ключевые вызовы и возможности для цифровой трансформации госкомпании включают также текущий уровень и потенциал роста цифровой зрелости госкомпании относительно лучших российских и международных практик и решений цифровой трансформации, как общих для всех отраслей, так и специфичных для отрасли. Ключевые вызовы и возможности должны формировать достаточную обосновывающую базу для выбора стратегических направлений цифровой трансформации.

Определение рисков и угроз информационной безопасности, которые могут возникнуть в ходе реализации цифровой трансформации при внедрении в деятельность госкомпаний современных цифровых технологий, сегодня, увы, является необходимостью. Как отмечают Falch и Henten (2018), при реализации цифровой трансформации госкомпаниями предстоит определение рисков (ущерба) и угроз информационной безопасности, связанных с внедрением современных систем связи.

При реализации цифровой трансформации госкомпаниям надлежит оценить риски (ущерба) и угрозы информационной безопасности, реализация которых может привести к негативным последствиям для деятельности госкомпаний, в том числе к нарушению функционирования и утечке защищаемой информации. При оценке рисков и угроз информационной безопасности должен учитываться текущий уровень использования современных цифровых технологий.

Риски и угрозы информационной безопасности должны формировать достаточную обосновывающую базу для выбора правовых, организационных и технических мер по обеспечению информационной безопасности в ходе реализации цифровой трансформации.

Для госкомпаний, являющихся субъектами критической информационной инфраструктуры Российской Федерации, определение рисков и угроз информационной безопасности должно осуществляться в соответствии с законодательством Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации.

Выработка целей цифровой трансформации госкомпании

Это направление цифровой трансформации может включать в себя такие направления работы как: создание целевой бизнес-модели, системы целей и ключевых показателей эффективности цифровой трансформации; определение стратегических направлений развития цифровой трансформации и горизонтов планирования стратегии цифровой трансформации.

Если опираться на достижения экономической теории и существующее правовое регулирование, целевая бизнес-модель должна включать описание целевой бизнес-модели госкомпании в контексте цифровой трансформации (или нескольких бизнес-моделей, если планируется использование более одной модели). При выборе целевой бизнес-модели учитывается текущее состояние и перспективы цифровой трансформации отрасли, уровень цифровой готовности (зрелости) госкомпании, ключевые возможности и вызовы для цифровой трансформации госкомпании.

Цели цифровой трансформации должны:

- быть ориентированы на повышение конкурентоспособности госкомпании;
- отвечать критерию экономической эффективности и включать оценку вклада цифровой трансформации в рост прибыли или другого аналогичного показателя госкомпании, а также оценку необходимых инвестиций в цифровую трансформацию и оценку их окупаемости;
- быть направлены (согласно сфере деятельности госкомпании) на достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления в соответствии с Указом Президента Российской Федерации от 21 июля 2020 г. № 474.

Каждой госкомпании желательно декомпозировать систему ключевых показателей эффективности цифровой трансформации, включив в нее три уровня: (1) вклад цифровой трансформации в стратегические цели госкомпании (включая увеличение прибыли или аналогичного показателя, увеличение выручки или аналогичного показателя, снижение затрат или аналогичного показателя); (2) цифровая трансформация ключевых сфер деятельности госкомпании — взаимодействие с потребителями, разработка и эксплуатация продуктов (для применимых отраслей), операции и цепочки поставок, поддерживающие функции (управление кадрами, управление финансами, управление закупками, управление зданиями и офисами и пр.); (3) обеспечение базовых корпоративных условий для цифровой трансформации — цифровая инфраструктура и система управления данными, кадры, компетенции и культура для цифровой трансформации, модель управления цифровой трансформацией.

Целевые значения ключевых показателей эффективности цифровой трансформации должны рассчитываться на основании текущих показателей госкомпании, ее стратегических целей, отраслевых и кросс-отраслевых сопоставлений («бенчмарков»).

Госкомпаниям следует выбирать стратегические направления цифровой трансформации на базе интегральной оценки по критериям потенциала вклада направления в достижение стратегических целей госкомпании и уровня готовности госкомпании к цифровой трансформации направления. В перечень направлений цифровой трансформации госкомпании рекомендуется

включать, но, не ограничиваясь, новую бизнес-модель (нескольких бизнес-моделей) и/или развитие дополнительных источников доходов, новые цифровые продукты и услуги, управление взаимоотношениями с потребителями, проектирование и инжиниринг, сервисное обслуживание, эффективность операций, управление цепочками поставок, управление кадрами, управление финансами, управление закупками. Для защиты информации, подлежащей защите в соответствии с законодательством Российской Федерации, необходимо использовать сертифицированные ФСБ России средства криптографической защиты информации (более подробно см. Постановление Правительства РФ от 30.06.2020 № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах»).

При планировании стратегии цифровой трансформации рекомендуется выделять три горизонта планирования: краткосрочный — примерно 12 месяцев (целевые значения для ключевых показателей эффективности устанавливаются с детализацией по времени на год, для ключевых показателей эффективности по импортозамещению устанавливаются на ежеквартальной основе); среднесрочный горизонт — 3–5 лет (целевые значения для ключевых показателей эффективности определяются также с детализацией по времени на каждый год); долгосрочный горизонт — 10 лет.

Каждый следующий горизонт должен развивать и расширять ключевые результаты и приоритетные направления цифровой трансформации предыдущего горизонта.

Разработка дорожной карты цифровой трансформации госкомпании

Это направление цифровой трансформации предполагает следующие направления развития:

- разработка и реализация инициатив по внедрению цифровых решений, по развитию цифровой инфраструктуры;
- развитие поставщиков цифровых решений;
- организационные мероприятия в рамках цифровой трансформации;
- мероприятия по программному импортозамещению;
- мероприятия по обеспечению информационной безопасности в рамках цифровой трансформации.

При планировании внедрения цифровых решений следует указывать полный перечень инициатив по направлениям цифровой трансформации, включая внедрение новых бизнес-моделей и развитие дополнительных источников доходов, взаимодействие с потребителями, операции и цепочки поставок, поддерживающие функции (управление кадрами, управление финансами, управление закупками, административно-хозяйственный отдел, юридическую службу и т. п.), а также по бизнес-направлениям и подразделениям госкомпании.

Желательно описывать применяемые подходы по выбору инициатив. При этом типовой подход включает формирование полного списка инициатив (на основании отраслевых практик, применимого опыта других отраслей, предложений от поставщиков и пр.) и отбор инициатив для внедрения (например, соответствие цифровой стратегии развития госкомпании, наибольший эффект для госкомпании, готовность инфраструктуры и др.).

Рекомендуется для каждой инициативы давать краткое описание, включая описание решаемой бизнес-задачи, описание внедряемого решения (используемые цифровые технологии), описание 5–10 ключевых вех реализации инициативы и определять сроки достижения каждой вехи, определять ответственное подразделение, другие подразделения головной компании и отдельные дочерние и зависимые общества.

Инициативы по развитию цифровой инфраструктуры должны включать описание требований к ИТ-инфраструктуре, ИТ-архитектуре, системе управления данными госкомпании, системе информационной безопасности и инструментам разработки цифровых решений (хранение кода, библиотеки разработки и т. п.). На основании требований к цифровой инфраструктуре и анализа ее текущего состояния формируется перечень инициатив по ее развитию с кратким описанием каждой инициативы (включая 5–10 ключевых вех реализации инициативы и сроки достижения каждой вехи, содержание работ, ответственное подразделение, операционные КПЭ, затраты).

Инициативы по развитию поставщиков цифровых решений должны включать определение ресурсов, которые будут задействованы при разработке и внедрении цифровых решений (собственные ресурсы или внешние поставщики); оценку объема работ для внешних поставщиков; установление подходов к работе с поставщиками (долгосрочная работа с ограниченным числом поставщиков и развитие их компетенций или выбор поставщика под каждую задачу и т. п.); программы и порядок работы со стартап-проектами; перечень инициатив по развитию поставщиков с кратким описанием каждой инициативы (включая 5–10 ключевых вех реализации инициативы и сроки достижения каждой вехи, ответственное подразделение).

По мнению Parfenova (2019), организационные мероприятия в рамках цифровой трансформации должны включать планируемые изменения в организационной структуре госкомпании в связи с цифровой трансформацией, создание центров цифровых компетенций, создание должности руководителя цифровой трансформацией (РЦТ, CDO/CDTO (Chief Digital Officer/Chief Digital Transformation Officer)), формирование его подразделения (офиса цифровой трансформации), описание функций, должностных обязанностей и полномочий. При этом желательно разрабатывать и утверждать перечень организационных мероприятий в рамках цифровой трансформации с кратким описанием каждого мероприятия (включая 5–10 ключевых вех реализации мероприятия и сроки достижения каждой вехи, ответственное подразделение).

Мероприятия по импортозамещению являются обязательной частью стратегии цифровизации любой госкомпании, включают перечень мероприятий, направленных на обеспечение перехода госкомпании на преимущественно использование российского программного обеспечения и радиоэлектронной продукции российского происхождения. Kirdina (2012) также отмечает, что госкомпаниям обязательны и мероприятия по обеспечению информационной безопасности в рамках цифровой трансформации, которые включают мероприятия, направленные на реализацию правовых, организационных, технических и иных мер обеспечения информационной безопасности. При этом выбор правовых, организационных, технических и иных мер обеспечения информационной безопасности должен быть направлен на предотвращение негативных последствий для деятельности госкомпаний, в том числе предотвращение нарушения функционирования информационной инфраструктуры госкомпаний и утечки защищаемой информации.

Госкомпаниям на уровне локальных правовых актов предписано устанавливать перечень мероприятий, направленных на реализацию правовых, организационных, технических и иных мер обеспечения информационной безопасности в рамках цифровой трансформации с кратким описанием каждого мероприятия (включая ключевые вехи реализации мероприятия и сроки достижения каждой вехи, ответственное подразделение). При этом ответственным подразделением за реализацию мероприятий по обеспечению информационной безопасности в рамках цифровой трансформации является подразделение по информационной безопасности госкомпаний.

Для госкомпаний, являющихся субъектами критической информационной инфраструктуры Российской Федерации, реализация мероприятий по обеспечению информационной безопасности в рамках цифровой трансформации осуществляется в соответствии с законодательством Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации.

Совершенствование «качества» кадрового состава госкомпании и формирование культуры цифровой трансформации

Это направление цифровой трансформации включает в себя деятельность по таким направлениям как:

- выработка модели цифровых компетенций и кадрового обеспечения цифровой трансформации госкомпании;
- оценка потребности в кадрах, обладающих специальной компетенцией;
- обучение цифровым навыкам и развитие цифровых компетенций сотрудников госкомпании;
- управление сотрудниками цифровых специальностей;
- планирование и проведение мероприятия по развитию цифровой культуры и культуры информационной безопасности госкомпании.

Моделирование цифровых компетенций и кадрового обеспечения цифровой трансформации госкомпании включает в себя: описание модели цифровых компетенций (или инициативы по внедрению модели цифровых компетенций); перечисление специальностей, востребованных в условиях цифровой экономики, с их описанием в терминах модели цифровых компетенций; расчет потребности в кадрах на основании портфеля инициатив цифровой трансформации с учетом стратегии компании по выбору поставщиков цифровых решений или внедрению цифровых решений собственными силами («сорсинг-модели»); привлечение кадров для реализации мероприятий по цифровой трансформации госкомпании (наем, развитие собственных кадров и пр.).

Обучение цифровым навыкам и развитие цифровых компетенций сотрудников госкомпании предполагает разработку образовательных программ и оценку численности сотрудников госкомпании для прохождения обучения компетенциям и технологиям, востребованным в условиях цифровой экономики.

Образовательные программы (курсы) госкомпании могут проводиться с использованием собственных ресурсов госкомпании или на базе сторонних образовательных учреждений. Для руководителей госкомпании желательно предусматривать отдельные программы обучения.

Как справедливо отмечают Kolychev et al. (2019), в перечень компетенций и технологий, которым обучается персонал, должны входить знания и навыки в области информационной безопасности. Перечень знаний и навыков в области информационной безопасности должен быть согласован с мероприятиями по обеспечению информационной безопасности.

Отдельного внимания заслуживает управление сотрудниками цифровых специальностей: особенности найма персонала; создание условий работы (например, особый график работы и условия работы в офисе); учет особенностей планирования карьеры (например, экспертные карьерные траектории); учет особенностей мотивации (например, усиление связи вознаграждения сотрудников госкомпании с результатами инициатив цифровой трансформации); особенности программ развития навыков и другие факторы.

Планирование и проведение мероприятия по развитию цифровой культуры и культуры информационной безопасности госкомпании включает в себя такие инициативы, как внедрение

клиентоориентированных подходов в работе, практик работы в условиях постоянно меняющихся требований (англ. *agile*) и дизайн-мышления, внедрение продуктоориентированного подхода в работе, сервисов обратной связи для сотрудников госкомпании, а также соблюдения организационных мер защиты информации и требований законодательства Российской Федерации, в том числе в части использования сертифицированных средств защиты информации.

Заключение

Произведя формально-юридический анализ нормативных актов в сфере цифровой трансформации госкомпаний, Gubin (2020), предлагает модель управленческого процесса — поэтапного внедрения цифровизации в деятельность некоммерческой организации, который в результате сможет повысить ее экономическую ликвидность.

Данная модель состоит из четырех основных этапов: анализа текущего состояния и перспективы цифровой трансформации госкомпании; выработки целей цифровой трансформации госкомпании; разработки дорожной карты цифровой трансформации госкомпании; совершенствовании «качества» кадрового состава госкомпании и формирование культуры цифровой трансформации.

Базой формирования оптимальной модели цифровой трансформации организации является проведение аналитических мероприятий по исследованию динамики спроса и предложения с появлением новых онлайн-платформ и цифровых экосистем, изменения в технологических векторах цифровой трансформации, изменения в качестве внешних условий для цифровой трансформации. При этом важным направлением выступает оценка рисков и угроз информационной безопасности, которая позволит сформировать оптимальную базу для выбора правовых, организационных и технических мер по обеспечению информационной безопасности в ходе реализации цифровой трансформации.

При этом выбор правовых, организационных, технических и иных мер обеспечения информационной безопасности должен быть направлен на предотвращение негативных последствий для деятельности госкомпаний, в том числе предотвращение нарушения функционирования информационной инфраструктуры госкомпаний и утечки защищаемой информации.

На основании вышеизложенного следует сделать вывод об особой юридической природе госкомпаний, которая совмещает в себе признаки юридического лица с государственным участием, но по своей экономической сути, представляет иную форму собственности (государственно-частную). То есть, фактически, государственные корпорации должны действовать наравне с остальными участниками рынка и не могут иметь каких-либо привилегий, за исключением привилегий, предусмотренных в целом для некоммерческих организаций. С другой стороны, с позиции правового регулирования (наличие отдельных федеральных законов, регламентирующих их деятельность), госкомпании безусловно становятся более «наглядными» для понимания государственной концепции внедрения цифровой трансформации.

References / Список литературы:

1. Álvarez Royo-Villanova, S. (2020). Digitalization: How will it work in practice? *ERA Forum*, *21*(2), 221–234. https://doi.org/10.1007/s12027-020-00607-9
2. Falch, M., & Henten, A. (2018). Dimensions of broadband policies and developments. *Telecommunications Policy*, *42*(9), 715-725. https://doi.org/10.1016/j.telpol.2017.11.004

3. Frolov, Yu., & Bosenko, T. (2020). The impact of armed conflict on economic performance and enterprise value in the country. *Economic Annals-XXI*, *182*(3-4), 49–55. https://doi.org/10.21003/ea.V182-06
4. Gubin, E. P. (2018). Pravovye aspekty povyshenija kachestva korporativnogo upravlenija v kompanijah s gosudarstvennym uchastiem [Legal aspects of the increase of corporate management quality in publicly-owned companies]. *Predprinimatel'skoe Pravo. Prilozhenie «Pravo i Biznes»*, (2), 35–40.
5. Karasev, A. T., Kozhevnikov, O. A., & Meshherjagina, V. A. (2019). Cifrovizacija pravootnoshenij i ee vlijanie na realizaciju otdel'nyh konstitucionnyh prav v RF [Digitalization of legal relations and its impact on implementation of particular constitutional rights of citizens in the Russian Federation]. *Antinomii*, *19*(3), 99–119. https://doi.org/10.24411/2686-7206-2019-10005
6. Kirdina, S. G. (2012). Rossijskie goskorporacii — Otvet na global'nye jekonomicheskie vyzovy [Russian state corporations — Response to global economic challenges]. *Akademicheskij Vestnik*, *2*(20), 184–188.
7. Kolychev, V. D., Belkin, I. O., & Udovidchenkov, R. S. (2019). Specifika i rezul'tativnost' programm razvitija upravlencheskih kompetencij kadrovogo rezerva [Specificity and effectiveness of the programs for the development of managerial competencies of personnel reserve]. *Vysshee Obrazovanie v Rossii*, (11), 134–143. https://doi.org/10.31992/0869-3617-2019-28-11-134-143
8. Parfenova, D. A. (2019). Gosudarstvennye korporacii i ih rol' v vozrozhdenii i modernizacii rossijskoj promyshlennosti (na primere gosudarstvennoj korporacii «Rosteh») [State corporations and their role in the revival and modernization of Russian industry (on the example of the state Corporation «Rostec»)]. *Via Scientiarum — Doroga Znanij*, (2), 40–45.
9. Tadayoni, R., Henten, A., & Sørensen, J. (2018). Mobile communications — On standards, classifications and generations. *Telecommunications Policy*, *42*(3), 253–262. https://doi.org/10.1016/j.telpol.2018.01.001
10. Williams, I., Falch, M., & Tadayoni, R. (2018). Internationalization of e-government services. *11th CMI International Conference, 2018: Prospects and Challenges Towards Developing a Digital Economy within the EU*, Article 8624828, 19–31. https://doi.org/10.1109/PCTDDE.2018.8624828

Сведения об авторах:

Савоськин А. В.* — доктор юридических наук, доцент, заведующий кафедрой конституционного и международного права Уральского государственного экономического университета, Екатеринбург, Россия.
savoskinav@yandex.ru
ORCID: 0000-0002-7112-6845

Рожкова Н. А. — магистрант Уральского государственного экономического университета, Екатеринбург, Россия.

Information about the authors:

Alexander V. Savoskin* — Dr. Sci. in Law, Associate Professor, Head of Constitutional Law Department, Ural State University of Economics, Ekaterinburg, Russia.
savoskinav@yandex.ru
ORCID: 0000-0002-7112-6845

Natalia A. Rozhkova — Master Student, Ural State University of Economics, Ekaterinburg, Russia.

https://doi.org/10.38044/2686-9136-2021-2-1-94-96

BOOK REVIEW

EVERYTHING IS DIGITAL: GETTING READY FOR THE INEVITABLE CHANGES

Slobodan Adžić

Faculty of Management, University of Union — Nikola Tesla
1a, Njegoseva, Sremski Karlovci, Serbia, 21205

For citation Adžić, S. (2021). Everything is digital: Getting ready for the inevitable changes. *Digital Law Journal, 2*(1), 94–96. https://doi.org/10.38044/2686-9136-2021-2-1-94-96

РЕЦЕНЗИЯ НА КНИГУ

ВСЕ ЦИФРОВОЕ: ГОТОВНОСТЬ К НЕИЗБЕЖНЫМ ПЕРЕМЕНАМ

С. Аджич

Факультет менеджмента, Союз университетов Никола Тесла
21205, Сербия, Сремски Карловцы, Негошева, 1а

Для цитирования Аджич, С. (2021). Все цифровое: готовность к неизбежным переменам. *Цифровое право, 2*(1), 94–96. https://doi.org/10.38044/2686-9136-2021-2-1-94-96

This essay reviews three books on business and society development in the context of industrialization and digitalization. The books are: *Digital Strategies in a Global Market — Navigating the Fourth Industrial Revolution* (Natalia Konina ed., 2021)[1], *Technology and Business Strategy — Digital Uncertainty and Digital Solutions* (Igor Stepnov ed., 2021)[2], and *Post-Industrial Society: The Choice between Innovation and Tradition* (Julia Kovalchuk ed., 2020).[3]

[1] Konina, N. (Ed.). (2021). *Digital strategies in a global market — Navigating the fourth industrial revolution*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-58267-8

[2] Stepnov, I. (Ed.). (2021). *Technology and business strategy — Digital uncertainty and digital solutions*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-63974-7

[3] Kovalchuk, J. (Ed.). (2021). *Post-Industrial society: The choice between innovation and tradition*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-59739-9

The authors of the book *Digital Strategies in a Global Market — Navigating the Fourth Industrial Revolution* (2021) research digital strategy as part of Corporate Business strategy. Digital strategy is characterized by the alignment of digital and business strategy and application of digital technologies and instruments to existing business activity along with the enablement of new digital capabilities to the core business. The authors research the different aspects of the creation and implementation of digital strategy, including digital strategic transformation, employing digital tools for innovations and new products research, sales reconfiguration and improvement, and firm digital technology architectures and processes.

It is stated that digital transformation is the central focal point behind the strategically driven process of changing a business in the face of new factors arising in the digital economy: changes can be planned through the introduction of a digital culture, the principles of customer-centricity, systematic work with innovations, adapting business models, the widespread use of data, and the development of competencies.

The authors of the book conduct systemic research into different aspect of digital strategy from the positions of business, as well as management and economy. This allows them to develop a comprehensive meta-scientific concept which states that digital strategy has vital significance for all sectors of economic activity. It is highly valuable that the authors propose scientific recommendations and a practical guide for various sectors of economy regarding the strategic adoption of digital tools, with emphasis on the role of digital marketing. The book also evaluates the opportunities and challenges of implementing digital strategy in the directions of more sustainable development and of the knowledge economy. The findings are convincing, concluding that managers should adapt their business strategy to a new digital reality. This mainly results in the digital adaptation of marketing, processes, and operations management.

This book can help readers to rethink how people, data, and processes interact, enabling companies to become more valuable to customers and gain a competitive edge in the digital-oriented world; it thus should appeal to those who are interested in digital strategies performance in global markets.

The book *Technology and Business Strategy — Digital Uncertainty and Digital Solutions* (2021) covers various aspects of the implementation of global technological leadership in the context of public policy in different countries, as well as individual companies and corporations. The book contains the results of a study into the transformation of competition in global markets, as well as the practical aspects of honing a competitive advantage in most markets (both known and emerging) for technologies, products, and services, including virtual and augmented reality, artificial intelligence, and others. The authors researched and systematized the principles and laws of the digital economy, the technological basis of future economic relations in the digital economy, changes in the structure of business models due to the widespread use of the platform approach, changes in the forms and content of corporate governance, the development of forms and methods of state regulation of digital manifestations, and changes in legislation and the financial sector.

It is useful that the book focuses on the uncertainty of future technologies, justifying the development not only of growth strategies but of also adaptation strategies; it also takes into account the risks and consequences of technological jumps. In addition, the book provides a comprehensive overview of the opportunities and challenges associated with developing global technology leadership strategies and would be an excellent resource both for researchers and for representatives of high-tech businesses interested in new competitive strategies in the emerging system of global technological leadership.

The book *Post-Industrial Society: The Choice between Innovation and Tradition* (2020) presents the results of research into the formation and functioning of post-industrial development institutions: development funds or banks in developed countries (USA, France, Norway, etc.) and developing countries (China, Russia, UAE, Indonesia, Vietnam, Kazakhstan, etc.). It is pointed out that, for all advanced and emerging economies that are simultaneously at the start of a breakthrough to a new technological order, a strategy for achieving target results should be reasonably chosen. This can be a strategy of reindustrialization based on the growth of industrial production (tradition), or a fundamentally innovative strategy of new industrialization (innovation).

Combining the work of recognized scientists and specialists in various academic fields, this book provides a comprehensive understanding of the aspects of post-industrial development, highlighting the driving forces and limitations, strategies, sources of funding, tools, and technologies for implementation. This book is pertinent to those readers who are interested in the specifics of implementing strategies for technological improvement in industry and the service sector in developed and developing countries.

As a result, the books under review represent comprehensive studies of the influence of new progressive technologies on business and society, including the formation of post-industrial society and digital economy. Moreover, their scientific and practical nature ensures their high theoretical and empirical value. These books indeed have made a valuable contribution to the fields of economics and management.

Information about the author:

Slobodan Adžić — Ph.D., Associate Professor, Faculty of Management, University of Union — Nikola Tesla, Sremski Karlovci, Serbia.
s.adzic@gmail.com
ORCID 0000-0002-8827-5492

Сведения об авторе:

Аджич С. — Ph.D., доцент факультета менеджмента Союза университетов Никола Тесла, Сремски Карловцы, Сербия.
s.adzic@gmail.com
ORCID 0000-0002-8827-5492