

DIGITAL LAW JOURNAL

Vol. 5, No. 2, 2024



ARTICLES

- 8** Digital Markets Act: A Hindrance to Innovation and Business Development
Kolawole O. Afuwape
- 24** Balancing the Interests of Users, Publishers and Developers in Cases of Shutdown of Video Games: A New European Initiative
Denis V. Graf
- 40** Big Data and Personal Data: Legal Nature and Regulatory Issues
Sanavbar N. Tagaeva, Elmira M. Gatiyatullina

REVIEW ARTICLES

- 53** Conceptual Approaches to Defining Digital Objects and Digital Assets
Anna G. Shipikova

BOOK REVIEWS

- 69** Regulating Artificial Intelligence: The Netherlands Project
Yuriy V. Volkov

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 5, No. 2, 2024

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 5, № 2, 2024



Contents

Articles

- 8** Digital Markets Act: A Hindrance to Innovation and Business Development
Kolawole O. Afuwape

- 24** Balancing the Interests of Users, Publishers and Developers in Cases of Shutdown of Video Games: A New European Initiative
Denis V. Graf

- 40** Big Data and Personal Data: Legal Nature and Regulatory Issues
Sanavbar N. Tagaeva, Elmira M. Gatiyatullina

Review Articles

- 53** Conceptual Approaches to Defining Digital Objects and Digital Assets
Anna G. Shipikova

Book reviews

- 69** Regulating Artificial Intelligence: The Netherlands Project
Yuriy V. Volkov

Содержание

Статьи

- 8** Акт о цифровых рынках Европейского союза: препятствие для инноваций и развития бизнеса
Колаволе Афувале
- 24** Баланс интересов пользователей, издателей и разработчиков при закрытии видеоигр в свете новой европейской инициативы
Денис Граф
- 40** Большие данные и персональные данные: правовая природа и вопросы регулирования
Санавбар Тагаева, Эльмира Гатиятуллина

Обзорные статьи

- 53** Подходы к определению цифрового объекта и цифрового актива
Анна Шипикова

Рецензии на книгу

- 69** Регулирование искусственного интеллекта: проект Нидерландов
Юрий Волков

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 manuscripts 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 Journal has been included in the index of the Higher Attestation Commission (VAK) of the Ministry of Education and Science of the Russian Federation. The subject of the journal corresponds to the group of specialties "Legal Sciences" and "Economic Sciences".

The journal publishes manuscripts in Russian and English.

FOUNDER, PUBLISHER:

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

EDITOR-IN-CHIEF:

Maxim I. Inozemtsev, Ph.D. in Law, Associate Professor, Department of Private International and Civil Law, Head of Dissertation Council Department of MGIMO-University, inozemtsev@digitallawjournal.org
76, ave. Vernadsky, Moscow, Russia, 119454

EDITORIAL BOARD

Alice Guerra — Ph.D. in Law and Economics, Associate Professor, Department of Economics, University of Bologna, Bologna, Italy

Max Gutbrod — Dr. jur., Independent Scientist, Former Partner and Managing Partner of Baker McKenzie, Moscow, Russia

Steffen Hindelang — Ph.D. in Law, Department of Law, University of Southern Denmark (University of Siddan), Odense, Denmark

Junzo Iida — Ph.D., Dean of the Graduate School of Law, Soka University, Tokyo, Japan

Anton A. Ivanov — PhD in Law, Associate Professor, Tenured Professor, School of Private Law, Academic Supervisor, Faculty of Law, HSE University, Moscow, Russia

Julia A. Kovalchuk — Dr. Sci. in Economics, Professor of the Department of Energy Service and Energy Supply Management, Moscow Aviation Institute, Moscow, Russia

Natalia V. Kozlova — Dr. Sci. in Law, Professor, Professor of the Department of Civil Law, Lomonosov Moscow State University, Moscow, Russia

Danijela Lalić — Ph.D. in Technical Sciences, Associate Professor, Faculty of Industrial Engineering and Management, Novi Sad University, Novi Sad, Serbia

Clara Neppel — Ph.D. in Computer Science, Master in Intellectual Property Law and Management, Senior Director of the IEEE European Business Operations, Vienna, Austria

Ludmila A. Novoselova — Dr. Sci. in Law, Professor, Head of the Department of Financial Transactions and New Technologies in Law, Russian School of Private Law, Private Law Research Centre, Head of the Department of Intellectual Rights, Kutafin Moscow State Law University (MSAL), Moscow, Russia

Francesco Parisi — Ph.D. in Law, Professor, Department of Law, University of Minnesota, Minneapolis, the USA

Vladimir A. Plotnikov — Dr. Sci. in Economics, Professor, St. Petersburg State University of Economics, St. Petersburg, Russia

Bo Qin — Ph.D., Professor, Head of the Department of urban planning and management, Renmin University of China, Beijing, China

Elina L. Sidorenko — Dr. Sci. in Law, Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics, Director of the Center for Digital Economics and Financial Innovations, Moscow State Institute of International Relations (MGIMO-University), Moscow, Russia

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, digitallawjournal.org , dlj@digitallawjournal.org
Published online:	28 June 2024
Copyright:	© Digital Law Journal, 2024
Price:	Free

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 рукописи 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 экономики 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.

Журнал включен в перечень ВАК по следующим специальностям: 5.1.1. Теоретико-исторические правовые науки (юридические науки), 5.1.3. Частно-правовые (цивилистические) науки (юридические науки), 5.1.5. Международно-правовые науки (юридические науки), 5.2.3. Региональная и отраслевая экономика (экономические науки), 5.2.4. Финансы (экономические науки).

В журнале публикуются рукописи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

Иноземцев Максим Игоревич

119454, Россия, Москва, просп. Вернадского, 76

ГЛАВНЫЙ РЕДАКТОР:

Максим Игоревич Иноземцев, кандидат юридических наук, доцент кафедры международного частного и гражданского права им. С. Н. Лебедева, начальник отдела диссертационных советов МГИМО МИД России, inozemtsev@digitallawjournal.org

119454, Россия, Москва, просп. Вернадского, 76

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Герра А. — Ph.D. in Law and Economics, доцент факультета экономики, Болонский университет, Болонья, Италия

Гутброд М. — Dr. jur., независимый исследователь, бывший управляющий партнер международной юридической фирмы Baker McKenzie, Москва, Россия

Иида Д. — Ph.D., декан Высшей школы по праву, Университет Сока, Токио, Япония

Иванов А.А. — кандидат юридических наук, доцент, ординарный профессор, департамент частного права, научный руководитель факультета права, Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

Ковальчук Ю.А. — доктор экономических наук, профессор, профессор кафедры энергетического сервиса и управления энергоснабжением, Московский авиационный институт, Москва, Россия

Козлова Н.В. — доктор юридических наук, профессор, профессор кафедры гражданского права, МГУ имени М.В. Ломоносова, Москва, Россия

Лалич Д. — Ph.D. in Technical Sciences, доцент факультета промышленной инженерии и менеджмента, Нови-Садский университет, Нови-Сад, Сербия

Неппель К. — Ph.D. in Computer Science (Technical University of Munich), Master in Intellectual Property Law and Management (University of Strasbourg), старший директор

по вопросам европейских бизнес-операций Института инженеров электротехники и электроники, Вена, Австрия

Новоселова Л.А. — доктор юридических наук, профессор, заведующий кафедрой финансовых сделок и новых технологий в праве, Российская школа частного права, Исследовательский центр частного права имени С.С. Алексеева при Президенте Российской Федерации, заведующий кафедрой интеллектуальных прав, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Москва, Россия

Паризи Ф. — Ph.D. in Law, профессор факультета права, Миннесотский университет, Миннеаполис, США

Плотников В.А. — доктор экономических наук, профессор, профессор кафедры общей экономической теории и истории экономической мысли, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия

Сидоренко Э.Л. — доктор юридических наук, доцент, профессор кафедры уголовного права, уголовного процесса и криминалистики, директор Центра цифровой экономики и финансовых инноваций, МГИМО МИД России, Москва, Россия

Хинделанг Ш. — Ph.D. in Law, факультет права, Университет Южной Дании (Сидданский университет), Оденсе, Дания

Цинь Б. — Ph.D., профессор, заведующий кафедрой городского планирования и управления, Университет Жэньминь, Пекин, Китай

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:	28.06.2024
Копирайт:	© Цифровое право, 2024
Цена:	Свободная

ARTICLES

DIGITAL MARKETS ACT: A HINDRANCE TO INNOVATION AND BUSINESS DEVELOPMENT

Kolawole O. Afuwape

O.P. Jindal Global University
Sonipat Narela Road, Jagdishpur Village, Sonipat, India, 131001

Abstract

The Digital Markets Act (DMA) is a significant regulatory effort of the European Union aimed at curbing the power of large tech companies and promoting fair competition in digital space. Despite its noble goals, there are growing worries about the negative impact it could have on innovation and entrepreneurship. This paper aims to determine the specifics of how the DMA could inadvertently impede innovation and discourage entrepreneurship. Through an analysis of the DMA's provisions, such as interoperability mandates and restrictions on self-preferencing, it is apparent that these stringent regulations could create significant barriers to entry for startups and discourage investment in emerging digital ventures. Additionally, the increased regulatory oversight mandated by the DMA could suppress willingness to take the risks necessary for entrepreneurial achievement, ultimately hindering the development of revolutionary advances. By thoroughly analyzing economic principles, real-world data, and relevant examples, this study clarifies the intricate relationship between regulation, innovation, and business in the digital realm. Furthermore, it suggests different regulatory strategies that aim to find a finer equilibrium between encouraging competition and fostering innovation, while highlighting the importance of customized structures that recognize the unique characteristics of digital markets. By shedding light on the possible compromises involved in the DMA, this research can be beneficial to policymakers and interested parties in order to facilitate scientific debates and regulatory choices regarding digital markets.

Keywords

Digital Markets Act, innovation, entrepreneurship, European Union regulations, restrictions, ex-ante, interoperability, self-preferencing, gatekeepers, data portability, fairness, antitrust, Digital Single Market, national competent authorities

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Afuwape, K. O. (2024). Digital Markets Act: A hindrance to innovation and business development. *Digital Law Journal*, 5(2), 8–23. <https://doi.org/10.38044/2686-9136-2024-5-2-3>

Submitted: 7 Apr. 2024, accepted: 16 May 2024, published: 28 June 2024

АКТ О ЦИФРОВЫХ РЫНКАХ ЕВРОПЕЙСКОГО СОЮЗА: ПРЕПЯТСТВИЕ ДЛЯ ИННОВАЦИЙ И РАЗВИТИЯ БИЗНЕСА

К. О. Афуване

Глобальный университет им. О. П. Джиндала
131001, Индия, Сонипат, п. Джагдишпур, ш. Сонипат Нарела

Аннотация

Акт о цифровых рынках Европейского союза (DMA) представляет собой важный шаг в ограничении власти крупных технологических компаний и содействии добросовестной конкуренции в цифровом пространстве. Несмотря на благородные цели данного акта, растет беспокойство по поводу его возможного негативного влияния на развитие инноваций и предпринимательской деятельности. В статье рассматриваются риски негативного влияния нового акта на инновационный и предпринимательский климат. Анализ требований к совместимости и ограничения на предоставление преимуществ собственным товарам показывает, что эти строгие правила могут создать существенные барьеры для входа стартапов и препятствовать инвестициям в новые цифровые предприятия. Кроме того, усиленный нормативный надзор, предписанный актом, может подавить готовность идти на риски, неотъемлемо присущие всякой предпринимательской инициативе, в конечном счете затрудняя развитие прорывных достижений. С учетом принципов развития экономики и опыта участников рынка автор проясняет сложную взаимосвязь между нормативным регулированием, инновациями и бизнесом в цифровой сфере. Кроме того, в работе предложены различные модели более тонкого и сбалансированного регулирования, направленные на поощрение конкуренции, стимулирование инноваций и учет уникальных характеристик отдельных цифровых рынков. Проливая свет на возможные компромиссные решения в толковании DMA, это исследование стремится способствовать развитию и углублению дискуссии о регулировании цифровых рынков.

Ключевые слова

акт о цифровых рынках, инновации, предпринимательство, регулирование Европейского союза, ограничения, ex-ante, совместимость, предоставление преимуществ собственным товарам, привратники, переносимость данных, справедливость, антимонопольное право, единый цифровой рынок, национальные антимонопольные органы

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имеет спонсорской поддержки.

Для цитирования

Афуване К. О. (2024). Акт о цифровых рынках Европейского союза: препятствие для инноваций и развития бизнеса. *Цифровое право*, 5(2), 8–23.
<https://doi.org/10.38044/2686-9136-2024-5-2-3>

Поступила: 07.04.2024, принята в печать: 16.05.2024, опубликована: 28.06.2024

Introduction

The Digital Markets Act (DMA)¹ marks a pivotal stride in curbing the dominance of tech giants and nurturing a more competitive digital environment.² The Digital Markets Act (DMA) is founded on the idea that competition law alone is not adequate to effectively handle the challenges and systemic issues brought about by the digital platform economy. Antitrust regulations are limited to specific cases of market power and anti-competitive behavior. Nevertheless, numerous substantial challenges pose a threat to its efficacy. The DMA could potentially worsen regulatory fragmentation in the European Union by allowing member states to interpret and implement its rules in varying ways, resulting in inconsistencies and inefficiencies.³ Additionally, the Act's wide-ranging responsibilities and restrictions may unintentionally lead to negative economic impacts, hindering innovation and disrupting market dynamics. Furthermore, the likelihood of legal conflicts due to uncertainties in the DMA's wording presents a significant obstacle, adding further complexity to its execution and regulation. The DMA needs to address provisions that are in conflict with current European regulations, which raises questions about its compatibility and consistency within the wider regulatory framework.⁴ This article explores all of these barriers, providing valuable perspectives on possible approaches to minimize their influence and improve the effectiveness of the DMA. By directly confronting these difficulties, policymakers can guarantee that the DMA achieves its desired goal of fostering competition, innovation, and consumer well-being in the digital era.

The initial objective of the DMA was to prevent regulatory fragmentation within the EU's Digital Single Market (DSM). However, it falls short of accomplishing this commendable objective, as it may cause member states to further increase regulatory fragmentation.⁵ The DMA's inclination towards

¹ Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 OJ (L 265).

² The Digital Markets Act (DMA), implemented by the European Union (EU), encompasses a series of regulations designed to diminish the influence of prominent technology companies to foster a more competitive landscape within European digital markets. These laws specifically target eliminating market obstacles erected by dominant «gatekeeper» platforms like Google, Facebook, and Amazon. See: Willige, A. (2023, September 19). *What does it mean for tech companies and consumers?* World Economic Forum. <https://www.weforum.org/agenda/2023/09/eu-digital-markets-act-big-tech/> — Regulations are introduced by the Digital Markets Act for platforms that serve as «gatekeepers» in the digital industry. These platforms impact the internal market significantly, operate as a vital conduit for corporate users to connect with their end customers, and currently hold, or will likely hold, a strong and long-lasting position. In addition to guaranteeing the openness of significant digital services, the Digital Markets Act seeks to stop gatekeepers from placing unjust restrictions on companies and end users. See also: European Commission. (2023, September 6). *Questions and answers: Digital Markets Act: Ensuring fair and open digital markets** https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349

³ See Teece, D. J., & Kahwaty, H. J. (2021). *Is the proposed Digital Markets Act the cure for Europe's platform ills? Evidence from the European Commission's impact assessment*. BRG Institute. <https://lisboncouncil.net/wp-content/uploads/2021/04/TEECE-AND-KAHWATY-Dynamic-Digital-Markets1.pdf> Here, the authors were of the view that a comprehensive evaluation of the provisions of the DMA would reveal that it is probable to exert a restraining influence on research and development (R&D) as well as innovation. This assertion is firmly grounded in fundamental economic principles. The stipulations of the DMA foster a culture of exploiting the investments made by others, thereby dissuading parties from undertaking such investments themselves. To safeguard Europe's capacity for innovation, it is imperative to prioritize the independent cultivation of dynamic capabilities.

⁴ Burwell, F. (2021, March 30). *Regulating platforms the EU Way? The DSA and DMA in transatlantic context*. Wilson Center. <https://www.wilsoncenter.org/article/regulating-platforms-eu-way-dsa-and-dma-transatlantic-context>

⁵ Portuese, A. (2022, August 24). *The Digital Markets Act: A triumph of regulation over innovation*. Information Technology and Innovation Foundation. <https://itif.org/publications/2022/08/24/digital-markets-act-a-triumph-of-regulation-over-innovation/>

pre-emptive regulatory actions and its focus on equity and constancy may inadvertently impede innovation. This prudent strategy has the potential to impede pioneering companies that aspire to disrupt prevailing market conventions.⁶ The DMA's emphasis on maintaining the existing status quo and ensuring fairness may prioritize stagnant competition, which depends on current market conditions, rather than dynamic competition that involves innovation and market advances.⁷ The favoritism could limit the opportunities for emerging players and creative business approaches. Giving more importance to disruption rather than fairness might hinder the ability of innovative companies to compete with established players and drive positive changes in the market. Long-term, this disparity may stifle competition and impede innovation.

The Digital Single Market (DSM) seeks to boost digital innovation, efficiency, and productivity throughout the European Union. Critics argue that the DMA could potentially impede these objectives rather than support them, as it may impose burdensome regulatory requirements on digital firms.⁸ Such requirements have the potential to suppress innovation and hinder gains in efficiency and productivity. The regulatory framework of the DMA is perceived as possibly burdensome for digital companies, potentially impeding their capacity to innovate and compete efficiently. Through the enforcement of stringent regulations and obligations, the DMA might establish obstacles for smaller entities looking to enter the market and discourage innovation (Bania, 2023, p. 116–149). The enforcement powers granted to individual EU member states under DMA's design result in a decentralized approach. This approach may result in regulatory fragmentation, as different countries may interpret and enforce the rules in varying ways (Bania, 2023, p. 116–149). Such fragmentation can create uncertainty for digital companies operating across borders and undermine the objective of achieving regulatory harmonization within the DSM.

The Digital Markets Act (DMA) has faced criticism for its per se prohibitions, with concerns raised about the lack of balance between pro-efficiency and pro-innovation justifications. Let us examine the specifics:

1. Prohibitions are regulations that categorize specific actions or behaviors as anti-competitive without the need for evidence of actual harm to competition. The criticism suggests that the DMA incorporates these prohibitions without considering efficiency or innovation. This inflexibility may fail to acknowledge complex scenarios where certain practices could genuinely enhance consumer welfare or foster innovation (Podszun, 2023).
2. The principle of proportionality necessitates that regulatory actions align with their intended goals and do not surpass what is essential to attain those goals (Podszun, 2023).⁹ If the DMA's inherent prohibitions lack valid reasons rooted in efficiency and innovation, they might contradict this principle. Consequently, this could result in excessive regulatory burdens on digital companies, potentially impeding innovation without satisfactory justification.

⁶ Lobo, S. (2024, March 15). *Apple opposes ex-ante regulations, similar to Digital Markets Act, in India*. Medianama. <https://www.medianama.com/2024/03/223-apple-digital-markets-act-ex-ante-regulations-india/>

⁷ See: Crémer, J. (2024, March 25). *Will the Digital Markets Act create a level playing field?* Toulouse School of Economics. <https://www.tse-fr.eu/Digital-Markets-Act>. The author was of the view that the leading technological platforms persist in their remarkable ability to foster innovation. Rather than questioning the extent of innovation achieved by today's platforms, the real inquiry lies in determining whether the level of innovation from both platforms and other companies would be greater and more tailored to the advantages of their users if they encountered heightened competition.

⁸ Broadbent, M. (2021, September 15). *Implications of the Digital Markets Act for transatlantic cooperation*. Center for Strategic and International Studies. <https://www.csis.org/analysis/implications-digital-markets-act-transatlantic-cooperation>

⁹ The principle of proportionality arises from the necessity to restrict governmental interference — through regulations, penalties, and supervision — to the extent required to accomplish the intended policy goals.

3. The DMA's imposition of rigid per se prohibitions, without taking into account the potential advantages in terms of efficiency or innovation, may result in higher compliance expenses for digital companies.¹⁰ Moreover, the inflexible nature of the regulatory framework could discourage companies from exploring innovative business strategies, due to concerns about potential legal consequences. Ultimately, this could stifle innovation within the digital sector.

The requirements of the DMA could potentially create uncertainty for businesses operating in the EU when they come into conflict with other EU regulations or directives. For example, if a company is required to comply with both the DMA and current data protection regulations, issues may arise regarding data sharing or processing procedures.¹¹ Conflicting demands could result in legal disputes and lawsuits as businesses strive to understand how to navigate the regulatory environment. These legal battles have the potential to prolong decision-making processes and raise compliance expenses for companies. Additionally, the uncertainty surrounding which regulations hold more weight may discourage innovative businesses from investing in the EU market due to concerns about potential legal liabilities. The possibility of maneuvering through intricate and possibly conflicting regulatory obligations might dissuade inventive enterprises from venturing into or enlarging their influence in the European Union market.¹² This could impede competition and restrict consumer options, ultimately hindering progress in the digital industry.

A Decentralized DMA

The decentralized enforcement of the DMA poses a threat to the DSM. In the course of discussions, the European Parliament introduced an amendment to Article 31a which establishes a “European High-Level Group of Digital Regulators” consisting of a Commission representative, a representative from pertinent Union entities, representatives from national competition authorities, and representatives from other National Competent Authorities (NCAs).¹³ The group is tasked

¹⁰ Bal, M., Debroy, B., & Ravi, S. (2022, November 25). *Devising an emerging market perspective for competition regulation in the digital age*. Observer Research Foundation. <https://www.orfonline.org/research/devising-an-emerging-market-perspective-for-competition-regulation-in-the-digital-age>

¹¹ The Digital Markets Act (DMA) seems to draw heavily from previous and current competition inquiries within the digital sector. The strategy of transforming solutions implemented for individual firms and business structures in particular market circumstances into universally applicable regulations poses challenges. This approach may lead to the regulation of practices that are not typically problematic and result in unintended consequences for business models that were not initially taken into account. See: Digital Europe. (2021, May 27). *Digital Markets Act position paper*. <https://www.digitaleurope.org/resources/digital-markets-act-position-paper/>

¹² Bal, M., Debroy, B., Gowda, R., & Ravi, S. (2022). *Devising an Emerging Market Perspective for Competition Regulation in the Digital Age*. ESYA Centre. <https://www.orfonline.org/public/uploads/posts/pdf/20230411144650.pdf> See also: Kavanagh, C. (2019, August). *New tech, new threats, and new governance challenges: An opportunity to craft smarter responses?* Carnegie Endowment for International Peace. <https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736>

¹³ According to G. Colangelo, recognizing the connection between competition law and the DMA, the European Competition Network (ECN) and certain EU member states (referred to as “friends of an effective DMA”) have put forward a suggestion to grant national competition authorities (NCAs) the authority to enforce DMA obligations. According to this proposal, the European Commission would retain its primary responsibility for enforcing the DMA and would have exclusive jurisdiction in designating gatekeepers or granting exemptions. However, NCAs would be authorized to enforce the obligations of the DMA and exercise investigative and monitoring powers at their discretion. See: Colangelo, G. (2022, March 23). *The Digital Markets Act and EU antitrust enforcement: Double & triple jeopardy*. International Centre for Law and Economics. <https://laweconcenter.org/resources/the-digital-markets-act-and-eu-antitrust-enforcement-double-triple-jeopardy/>

with guiding the Commission on the integration of national competition authorities (NCAs) in the decentralized enforcement of the DMA. Article 31c, as introduced by the European Parliament, reinforces this by outlining the responsibilities of NCAs and other relevant authorities. It specifies that NCAs are required to assist the Commission in overseeing adherence to and implementation of the rules outlined in this Regulation. Thus, the DMA will be under the control of the NCAs, leading to decentralized enforcement and contradicting the aim of reducing regulatory fragmentation. The coalition is also in favor of allowing firms to engage in “private” enforcement of the DMA, which means that they should have the ability to take legal action against gatekeepers to uphold their obligations. This perspective is based on the belief that private enforcement will enhance the DMA’s efficiency, but it could lead to attempts by dominant competitors to suppress competition and hinder innovation.¹⁴ Pressure exerted by influential states within the Friends of an Effective Digital Markets Act coalition have yielded positive results. Margrethe Vestager, the Executive Vice President of the European Commission, is now advocating for the involvement of national authorities in enforcing the DMA.¹⁵ Germany is already demonstrating its authority and impact in shaping the implementation of the DMA.¹⁶

Member states have been actively advocating for a redistribution of enforcement responsibilities among the NCAs in the latest version of the DMA, giving them a more significant role. The EU institutions have successfully reached a political consensus leading to a thorough revision of Article 31d (1) of the DMA.¹⁷ Originally proposed by the European Parliament, the above provision established certain constraints and obligations on the involvement of Member States in the enforcement of the DMA. Article 32a (6) of the most recent edition of the DMA allows NCAs to directly enforce the DMA without resorting to the covert application of national competition regulations. This provision explicitly states, “If a competent authority of a Member State has the necessary jurisdiction and investigative authority under national legislation, it may independently investigate a potential violation of Article 5, 6, and 6a of this Regulation within its jurisdiction.”

¹⁴ Colangelo, G. (2022, March 23). *The Digital Markets Act and EU antitrust enforcement: Double & triple jeopardy*. International Centre for Law and Economics. <https://laweconcenter.org/resources/the-digital-markets-act-and-eu-antitrust-enforcement-double-triple-jeopardy/>

¹⁵ According to Margrethe Vestager, “What we want is simple: Fair markets also in digital. We are now taking a huge step forward to get there — that markets are fair, open and contestable. Large gatekeeper platforms have prevented businesses and consumers from the benefits of competitive digital markets. The gatekeepers will now have to comply with a well-defined set of obligations and prohibitions. This regulation, together with strong competition law enforcement, will bring fairer conditions to consumers and businesses for many digital services across the EU.” See: European Commission. (2022, March 25). *Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978

¹⁶ Kabelka, L. (2022, April 12). *DMA: Germany the test bench for complementarity with competition authorities*. Euractiv. <https://www.euractiv.com/section/digital/news/dma-application-could-lead-to-legal-uncertainty-in-germany/> Section 19a of the Act against Restraints of Competition (ARC) in Germany is commonly known as the DMA’s blueprint, mainly due to its comparable scope of application. See: Secure Privacy. (2023, December, 23). *A comparison of the German Competition Act (GWB) and the Digital Markets Act (DMA)*. <https://secureprivacy.ai/blog/german-competition-act-digital-markets-act-comparison>

¹⁷ Carugati, C. (n. d.). *The role of national authorities in the Digital Markets Act*. Jean Monnet Network on EU Law Enforcement Working Paper Series No. 34/22. <https://jmn-eulen.nl/wp-content/uploads/sites/575/2022/05/WP-Series-No.-34-22The-Role-of-National-Authorities-in-the-Digital-Markets-Act-Carugati.pdf>

The duty of the relevant NCA to inform the Commission of any investigation is the only requirement for the unilateral and local enforcement of the DMA's obligations and prohibitions.¹⁸ The latest version of the DMA enables decentralized enforcement without imposing any major restrictions, which is in line with the recommendations made by the Friends of an Effective Digital Markets Act.¹⁹ Nevertheless, due to the absence of coordination, decentralized enforcement of the DMA at the EU level may prove to be less efficient, leading to an increased likelihood of judicial actions at the national level. This could also weaken the legal foundation for NCAs to enforce a regulation primarily created to eliminate regulatory fragmentation.

Non-Acknowledgment of Legitimate Justifications by the DMA

The DMA's arbitrary line-drawing rules concerning size thresholds and qualitative criteria for identifying 'gatekeepers' lack economic rationale. This results in the unequal treatment of firms with comparable market positions solely based on their inclusion within the DMA's scope (Podszun, 2023). The DMA fails to provide clear definitions of markets and overlooks essential concepts of competition law, such as 'market dominance'. As a result, companies that are not dominant will be subject to the new competition rules, while certain dominant companies will be exempt from them. This presents a paradox within the DMA, as it may potentially scrutinize market challengers more rigorously than incumbents. Recital 5 of the DMA indicates that designated gatekeepers may not necessarily be dominant in terms of competition law. This is because digital marketplaces typically have a large number of players, complex ecosystems, and fast innovation. In these situations, a single company may have significant control over important infrastructure or services, even if it does not strictly meet the definition of dominant. It is possible that the power dynamics found in digital marketplaces are not fully reflected by conventional measures of dominance, such as market share or entrance obstacles.

The DMA contains size thresholds that are highly questionable, and the regulation itself is harmful because it establishes ex-ante rules that are essentially prohibitions. It is undeniable that attaining market supremacy in the digital economy requires exceptional efficiency. It is important to remember that users are just as eager to take advantage of network effects. However, having less competition can negatively impact customers, who might have had to make fewer compromises in terms of privacy in a more competitive market. The only ways to promote competitiveness in the absence of interoperability are through legislation or disruptive innovation

¹⁸ According to the Centre on Regulation of Europe, there are mechanisms in place to facilitate the collaboration between the enforcement of the DMA and competition law. It is mandatory to ensure that all relevant authorities are kept up to date on enforcement actions and that confidential data can be exchanged between different entities. Specifically, (i) if a National Competition Authority (NCA) plans to initiate an investigation on one or more gatekeepers according to national legislation, it must notify the Commission and may also inform other NCAs; (ii) if an NCA intends to impose obligations on gatekeepers based on national law, it must share the proposed measures with the Commission, even if they are temporary measures. The information exchanged is solely to coordinate enforcement efforts. See p. 184 in De Streel, A., Borreau, M., Micova, S. B., Feasey, R., Fletcher, A., Kraemer, J., Monti, G., & Pietz, M. (2023). *Effective and proportionate implementation of the DMA*. Centre on Regulation of Europe. https://cerre.eu/wp-content/uploads/2023/01/DMA_Book-1.pdf

¹⁹ Rurali, G., & Seegers, M. (2023, June 20). *Private enforcement of the EU Digital Markets Act: The way ahead after going live*. Kluwer competition law blog. <https://competitionlawblog.kluwercompetitionlaw.com/2023/06/20/private-enforcement-of-the-eu-digital-markets-act-the-way-ahead-after-going-live/>

which, in itself, is anti-innovative and capable of stifling business development and enterprise.²⁰ Nevertheless, rules of reason, which allow for legitimate justifications to be weighed against regulatory obligations, are more effective for avoiding incorrect judgments and identifying practices that promote competition. The blanket prohibitions under the DMA that are imposed on designated gatekeepers cannot be challenged by the gatekeepers' economic justifications. The DMA will only consider exceptions that are grounded in "public morality, public health, or public security." As a result, practices that are prohibited are assumed to hurt competition regardless of any efficiency arguments put forth by the defendant, such as enhancing consumer welfare or product innovation through technological advancement (Monti, 2022, p. 40–68). The transition from ex-post antitrust enforcement to ex-ante regulatory measures mirrors the implementation of the precautionary principle in antitrust cases: regulatory interventions at an early stage aim to deter harmful practices and uphold the current state of affairs.

Over or Under Enforcement of the DMA?

It is challenging for any regulatory framework to achieve the ideal degree of enforcement. Excessive enforcement can hinder creative thinking and productive enterprises. The objectives of the regulating legislation may be compromised by inadequate enforcement. It is difficult to forecast whether there will be systematic over- or under-enforcement.²¹ Today, it is believed that the "more economic approach" contributed to a more cautious antitrust enforcement strategy that would be partially replaced by the DMA. It is nearly impossible to conduct a thorough study of the DMA's effects on enterprises and innovation ahead of time given the variety of responsibilities involved.

The equilibrium between over- or under-enforcement is not solely determined by matters of substance, but also by the enforcement regime and its institutional framework (Knapstad, 2023, p. 394–409). The data protection regulations in the EU, although comprehensive in terms of substance, serve as an illustration of inadequate institutional design. The European Commission is designated as the exclusive enforcement authority for the Digital Markets Act (DMA), with agencies from EU Member States limited to assisting. The internal structure of the European Commission will need to address key considerations such as staffing levels dedicated to DMA enforcement, the expertise of case handlers, their motivations, and the extent of judicial oversight over their rulings.²² These factors will play a crucial role in shaping the effectiveness of enforcement actions. Private individuals have the option to initiate legal proceedings against gatekeepers through private enforcement, leading to a substantial enhancement in the enforcement measures.²³ It is widely acknowledged that private enforcement can be pursued in domestic courts, even though the provisions concerning this aspect in the DMA are notably inadequate. Users have the right to

²⁰ Heimann, F. (2022, June 13). The Digital Markets Act — We gonna catch 'em all? Kluwer competition law blog. <https://competitionlawblog.kluwercompetitionlaw.com/2022/06/13/the-digital-markets-act-we-gonna-catch-em-all/>

²¹ European Commission. (2023, September 6). *Questions and answers: Digital Markets Act: Ensuring fair and open digital markets** https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349

²² The enforcement of digital competition rules against big tech will be carried out by the European Commission, which should internally guarantee a dedicated process and teams. See: Martins, C., & Carugati, C. (2022, May 11). *Insights for successful enforcement of Europe's Digital Markets Act*. Bruegel. <https://www.bruegel.org/blog-post/insights-successful-enforcement-europes-digital-markets-act>

²³ Margvelashvili, T. (2023, December 14). Tracing forum shopping within the DMA's private enforcement: Seeking equitable solutions. Kluwer competition law blog. <https://competitionlawblog.kluwercompetitionlaw.com/2023/12/14/tracing-forum-shopping-within-the-dmas-private-enforcement-seeking-equitable-solutions/>

file lawsuits seeking cease-and-desist orders, interim relief, and potentially even compensation for damages incurred.²⁴

The Negative Impacts of Ex-Ante Regulations

Article 5(1) prohibits self-preferential practices, despite their prevalence in the business world, which often stimulate competition, drive innovation, and improve consumer welfare.²⁵ However, the DMA unequivocally bans these practices, including tying, bundling, and leveraging strategies, despite their positive effects on competition and innovation (Hornung, 2024, p. 396–437). The prohibition will have a substantial impact, negatively affecting consumers and numerous businesses within the gatekeepers' network that rely on and benefit from their services and products. These restrictions may also result in a significant deterrent effect. Platforms that are not gatekeepers may perceive such behaviors as potentially anticompetitive according to regulators, even though the DMA might not place any limitations on them (Andriychuk, 2023, p. 123–132). In reality, the DMA's automatic bans on supposedly 'unfair' practices will impact the entire economy, as the DMA could ultimately be invoked in conventional competition lawsuits (Bostoen, 2023, p. 263–306). The per se prohibition rules of the DMA are expected to have an impact on innovation, consumer welfare, and the choices available to both consumers and business users. These rules lack economic justification and may result in a decrease in innovation, a decline in consumer welfare, and limited options for consumers and businesses (Deutscher, 2022, p. 302–340). The DMA purportedly seeks to prevent the "extreme nature of unjust practices." However, the DMA is ultimately likely to prohibit and discourage practices that promote competition and innovation, such as self-preferencing, data aggregation, data merging, and leveraging strengths that may impact consumer well-being and innovation (Cennamo et al., 2023, p. 44–51).

The EU principle of proportionality may be violated by blanket prohibitions on potentially pro-competitive practices, as these prohibitions are not specifically designed to address unfair practices, which goes against the claims of the DMA (Lamadrid de Pablo & Bayón Fernández, 2021, p. 576–589). To ensure reasonableness, EU judges have the authority to reduce the set of obligations and prohibitions imposed by the DMA. The ex-ante rules of per se prohibitions implemented by the DMA are an unfavorable policy that greatly hinders the principles of fair competition and disregards the fundamental legal principles of the EU's legal order (Colangelo, 2023, p. 538–556). A more rational approach would involve the application of the rule of reason, where judges assess the positive and negative impacts of the rules through a balancing test. In the end, it is likely that EU judges will inevitably embrace this approach when adjudicating the DMA.²⁶

The implementation of the DMA is expected to exacerbate an already intricate regulatory structure, leading to more disorder. As an illustration, the DMA compels gatekeepers to separate essential

²⁴ The DMA's endorsement of private enforcement is additionally demonstrated in Article 42 and Recital 104, particularly emphasizing consumer rights. Consumers are enabled to pursue their claims against gatekeepers' obligations through representative actions that are consistent with Directive (EU) 2020/1828. See: Directive 2020/1828, of the European Parliament and of the Council of 25 November 2020 on Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive 2009/22/EC, 2020, OJ (L 409). <https://eur-lex.europa.eu/eli/dir/2020/1828/oj/eng>

²⁵ The general obligations of gatekeepers are specified in Articles 5 and 6 of the DMA. Article 6(5) specifically addresses the issue of self-preferencing. See p. 7 in Peitz, M. (2022, November). *The prohibition of self-preferencing in the DMA*. Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2022/11/DMA_SelfPreferencing.pdf

²⁶ Bauer M., Erixon, F. Guinea, O. van der Marel, E., & Sharma, V. (2022, February). The EU Digital Markets Act: Assessing the quality of regulation. European Centre for International Political Economy. <https://ecipe.org/publications/the-eu-digital-markets-act/>

platform services from each other. According to Article 5(f) of the DMA, gatekeepers are obligated to abstain from mandating that business users or end-users avail themselves of additional core platform services to utilize, access, or register for any of the core platform services specified under that Article.²⁷ The provisions of the DMA that mandate unbundling will hinder gatekeepers from adhering to Article 7 of Directive 2019/770, which requires platforms to provide a detailed description of the functionality and interoperability of their primary platform services.²⁸ This is because the DMA also permits other business users to modify the original functionality and interoperability of any core platform service, thereby rendering it practically impossible for gatekeepers to possess comprehensive knowledge of the interoperability and functionality of their services. The DMA establishes data portability rights for business users about gatekeepers.²⁹ However, these rights could potentially infringe upon the privacy rights of end-users protected under the GDPR³⁰. According to Article 6(i) of the DMA, gatekeepers are required to:

“provide business users and third parties authorized by a business user, upon their request, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services offered together with or in support of the relevant core platform services by those business users and the end users engaging with the products and services provided by those business users; for personal data, provide access and use only where the data are directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform services, and when the end-user opts into such sharing by their consent.”

The DMA imposes an obligation on the gatekeeper to transfer data to a business user once the end-user has given consent to such sharing.³¹ However, following a one-time blanket approval by the end-user upon initial registration with the business user, the business user may obtain an excessive amount of personal data from gatekeepers. The sharing of this data could occur without the end users being completely informed that the data produced while utilizing the gatekeepers’

²⁷ The Digital Markets Act establishes an equitable digital landscape by defining rights and regulations for major online platforms (known as ‘gatekeepers’) and guarantees that gatekeepers do not exploit their dominant position. By overseeing the digital market on a European Union scale, it fosters a just and competitive digital atmosphere, enabling both businesses and customers to take advantage of digital advancements (<https://www.eu-digital-markets-act.com/>).

²⁸ Directive 2019/770, of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, 2019 OJ (L 136).

The gatekeeper must ensure that the fundamental features of its number-independent interpersonal communications services are compatible with those of another provider in the EU, either already providing or planning to provide such services. This can be achieved by offering technical interfaces or other solutions that promote interoperability, without any additional cost (Article 7). See: Małobęcka-Szwast, I. (2023, August 24). *The Digital Markets Act: A revolution, and not only for gatekeepers*. Lexology. <https://www.lexology.com/library/detail.aspx?g=1417472a-4597-4ea3-9925-0a7060aafbde>

²⁹ The DMA defines “interoperability” as “the ability for hardware and software elements to work with other hardware and software elements and with users in all how they are intended to function, and to mutually use the information which has been exchanged through interfaces or other solutions” (Art. 2(29)). Vertical (Art. 6(4), (7)) or horizontal (Art. 7) interoperability is possible.

³⁰ Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to The Processing of Personal Data and On the Free Movement of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ (L 119).

³¹ Usercentrics. (2024, January 18). How the European Digital Markets Act (DMA) impacts user privacy and consent management. <https://usercentrics.com/knowledge-hub/digital-markets-act-dma-impacts-user-privacy-and-consent-management/>

services will eventually be owned by numerous business users. Consequently, this situation is likely to contradict the GDPR, which requires the consent of end users to process their data. Article 7(4) prohibits the excessive processing of personal data for contract performance. Despite this, the DMA gatekeeper may mandate gatekeepers to disclose data to business users that goes beyond what is essential to deliver the requested services. Simultaneously, the DMA could potentially clash with the data portability stipulations outlined in the GDPR (Turner & Tanczer, 2024). The DMA specifically pertains to the disclosure of data that is “directly linked to the actions taken by the end-user about the products or services provided by the respective business user.” The interpretation of the term “directly connected” has yet to be established by regulatory bodies and judicial authorities through practical application. Nevertheless, imposing limitations on the types of data that can be transferred may prompt gatekeepers to breach Article 20 of the GDPR, which governs the portability of personal data. This provision entitles individuals to transfer their data from one data controller to another “without hindrance”.

The gatekeeper must choose between adhering to Article 6(i) of the DMA, which restricts data portability of personal data and may lead to a breach of Article 20 of the GDPR, or enabling data portability “without hindrance” in accordance with Article 20 of the GDPR, which could result in a violation of Article 6(i) of the DMA. The DMA encompasses numerous obligations, such as Article 6(i), which may potentially clash with the data protection regulations of the European Union.

The Digital Markets Act (DMA) may also come into conflict with requirements outlined in the Digital Services Act (DSA). For example, while Article 5 of the DSA mandates that online platforms must promptly remove or disable access to illegal content to avoid liability, Article 6(1)(k) of the DMA stipulates gatekeepers must ensure fair, reasonable, and non-discriminatory conditions of access for business users to their software application store, online search engines, and online social networking services. Essentially, gatekeepers are obligated to offer fair treatment to all business users. The outcome of these regulatory challenges leads to the emergence of gatekeepers who will embrace a more cautious stance towards innovation in order to mitigate their legal liabilities. Unfortunately, this approach will ultimately have detrimental effects on consumers and hinder overall economic progress.

Findings

As intended by the EU, the DMA lays out rules for larger digital platforms classified as ‘gatekeepers’ to promote fair competition and prevent anti-competitive practices. While this is a noble aim, the DMA creates several difficulties on the legal front, especially with respect to conflicts between laws. Conflicts arise from differing regulatory environments and extraterritorial impacts, as well as innovation-compliance rifts. An extensive analysis of the nature and essence of those conflicts is presented here. Though the DMA’s ambitious goal of ensuring fairness in digital markets and reducing the dominance of gatekeepers is to be warmly commended, it is shadowed by complex legal panoramas. The conflicts between laws would arise from differing regulations, extraterritorial effects, and constraints on innovation. An approach that specifically reflects the other angles of harmonization, cooperation, and adaptability would allow for the resolution of such conflicts without compromising the fairness and competitiveness of that global digital ecosystem.

Divergent Regulatory Approaches

The DMA sets stringent guidelines that contrast with the more laissez-faire approach of other jurisdictions, such as those exhibited in the United States and China. For example, in US antitrust law, actions that damage the interests of consumers are prioritized, with a focus on pricing and quality, while the DMA is oriented towards fair competition and markets. In China, the primary focus in regulating digital markets is on ensuring government control and data sovereignty, while they are minimally regulated for competition.

Discrepancies between the regulations of individual jurisdictions may lead to challenges for multinational businesses that operate in a number of them due to inconsistent compliance requirements.

Impact on Multinational Gatekeepers

With so many countries requiring different considerations/guidelines that may be less restrictive or somewhat contradictory, multinational firms like Google, Apple, and Amazon face compliance conflicts with the DMA within their ecosystem, leading to operational inefficiencies, and possibly to litigation.

Extraterritoriality and Jurisdictional Overreach

The DMA carries international implications, as it applies not only to EU gatekeepers, but those located outside of the EU that conduct business in its market.

Conflict with Principles of Sovereignty: the DMA may be perceived as encroaching upon the sovereignty rights of non-EU nations by extending its regulations to foreign enterprises. An illustrative example would be:

A gatekeeper based outside of the EU could be penalized under the DMA for conduct that might be lawful in its home country. This establishes a complex tension between international trade and digital diplomacy, which may result in potential retaliatory measures and trade conflicts.

Dual Compliance Burden: companies that operate in more than one jurisdiction are necessarily made to comply with overlapping or contradictory rules.

For example, a data-sharing obligation from the DMA could violate data privacy requirements imposed by the USA Cloud Act or the Data Security Law of China, resulting in various legal quandaries.

Innovation vs. Regulation

Chilling Effect on Innovation:

Innovation: Restrictions on self-preferencing, demands for interoperability, and forced data sharing under the DMA may chill, if not freeze, innovation altogether.

Companies may think twice about the costs and time involved in launching new products and services to the market if caught up in regular DMA compliance disputes.

As with small businesses that are dependent on various platforms run by gatekeepers, startups may have fewer investment opportunities considering the demand for tighter operational scrutiny.

Misalignments in Global Standards

Due to compliance with the DMA, gatekeepers might amend their platforms and business models, which may inhibit their ability to innovate on a global scale. An example is given below:

The interoperability mandated by the DMA might conflict with US market protections for proprietary technologies, thereby creating disincentives for investments in research and development.

Conflict between EU member states and the EU framework

National vs. EU-Level Regulation:

The DMA is supposed to bring about harmonization, but conditions may arise that create conflicts between the DMA and national competition or consumer protection:

Some EU member states may develop their own national regulations that are stricter than those outlined in the DMA, thus introducing fragmentation.

Companies must operate under both the DMA and diverse national regulations, bolstering an increase in their legal liabilities and compliance costs.

Inconsistencies in Enforcement:

The European Commission is designated as the sole enforcement authority under the DMA, but different national authorities may have different views on compliance, which could lead to disputes and inconsistent application of rules.

Sectoral and Industry Conflicts

Sectoral Regulations vs. DMA:

Certain sectors, like finance and health, are more stringently controlled than others. Their broad mandates could possibly conflict with those put in place by sector-specific laws.

Interoperability demands for gatekeepers may at times collide with banking secrecy laws within finance.

Health organizations may have difficulty reconciling DMA requirements with GDPR privacy requirements.

Impact on SMEs and Startups

In implementing the DMA with the objective of protecting small firms, some provisions might fortuitously erect barriers:

Difficulties that deprive gatekeepers of the ability to give start-ups platform access, hence challenging the submission of such start-ups, may eventually limit market entry and innovation.

International Trade and Economic Relations

Trade Conflicts and Retaliation:

This module on the scope of the DMA might elicit retaliation from non-EU countries, especially the US, which is where most of these gatekeepers are based. This could end up as a dire global trade war that hampers overall digital trade.

Fragmentation of Digital Markets:

One of the many ways the DMA might affect digital markets is by having different regional solutions developed by gatekeepers to meet conflicting legal requirements, thereby undermining global integration and innovation.

Recommendations for Resolving Conflicts Between Laws

- Harmonization of Global Standards:
 - Encourage a new international dialogue and cooperation through institutions like the World Trade Organization (WTO) and the Organization for Economic Cooperation and Development (OECD) to identify commonalities within regulations dealing with competition and digital markets.

- Establishment of a global framework for the regulation of digital markets that respects regional specifics while minimizing potential conflicts.
- Clarification of Jurisdictional Boundaries:
 - The DMA should have clearer limits for its extraterritorial applicability to avoid disputes over sovereignty and to minimize legal uncertainties.
 - Mutual agreements with third-party states to prevent inconsistencies between respective regulatory frameworks should be proposed.
- Flexible and Adaptive Frameworks:
 - The DMA must incorporate provisions for the review and adjustment of regulations to address evolving technological and market dynamics.
 - The European Commission ought to allow for industry-specific exemptions or adjustments that reduce conflicts with current regulations.
- Collaborative Compliance Models:
 - Encourage joint compliance initiatives that engage gatekeepers, national authorities, and the European Commission in order to streamline enforcement and minimize disputes.
 - Introduce a mechanism for cross-border dispute resolution that would address disputes arising from jurisdictional conflicts.

Conclusion

As stated in Article 1(1), the DMA aims to enhance the internal market by establishing uniform regulations. However, it falls short of this goal. Instead of solely fostering the beneficial impact of European regulation on digital markets, the DMA allows for various national regulatory actions, maintains barriers to online operations, and increases the likelihood of inconsistent enforcement measures. Article 1(6) specifies that Member States have the authority to establish additional regulations and requirements for gatekeepers, provided they relate to “national competition rules.” Since the DMA introduces new competition rules and Member States can add further competition rules for gatekeepers, this will likely result in greater regulatory fragmentation.

The Digital Markets Act (DMA) diverges from modern competition law by placing less emphasis on economic evidence and concepts. This shift suggests that economic reasoning may not align seamlessly with the current legal framework for evaluating individual cases. Nevertheless, economics continues to play a significant role in shaping legislation at a broader level. The creation and enforcement of the DMA will introduce regulatory ambiguity. Gatekeepers will need to determine whether to adhere to the DMA or other EU regulations, such as the GDPR. This uncertainty will further hinder covered platforms’ capacity to innovate and promote consumer welfare. The DMA’s prohibition of practices that could potentially promote competition may impede economic progress and harm consumer well-being. This issue is compounded by the lack of adequate economic reasoning behind these restrictions, potentially breaching EU principles of proportionality. Judges will need to address conflicts between the DMA and the principle of proportionality, potentially limiting future DMA enforcement.

The DMA is nearing its final stages of adoption by EU institutions, but significant concerns remain regarding its approval and enforcement. As noted earlier, the primary objective of the DMA is to address regulatory fragmentation within the EU’s Digital Single Market (DSM). Regrettably, it falls short of achieving this goal, as it inadvertently encourages Member States to exacerbate regulatory fragmentation.

The shift in the DMA from ex-post to ex-ante rules, using per se antitrust prohibitions, fails to differentiate between conduct that fosters competition and conduct that hinders it. Consequently, the DMA overlooks the benefits of economic efficiency and conflicts with the EU's principle of proportionality. Implementing the DMA is expected to pose challenges, particularly for the limited number of companies identified as Internet gatekeepers, who will need to comply with rules that may contradict other existing EU regulations.

To address these concerns, it is essential to establish a regulatory framework for the DMA that effectively targets anti-competitive behavior while fostering efficiency and innovation. This can be achieved by incorporating mechanisms to evaluate the positive competitive effects of specific practices and allowing exceptions to absolute prohibitions when efficiency or innovation justifies them. Such an approach would ensure the DMA adheres to the EU's principle of proportionality while minimizing adverse effects on competition and innovation.

EU lawmakers must address the deficiencies in the legislation, possibly by introducing enforcement guidelines. At the same time, EU judges will need to harmonize the obligations of the DMA with other rights provided under EU laws. If these fundamental issues are not resolved by lawmakers or judges, European innovation and consumers will undoubtedly suffer adverse effects. Policymakers should conduct a thorough review of the DMA's provisions to align them with existing EU laws, addressing concerns that the DMA could stifle innovation and discourage enterprise. Establishing clear guidelines and mechanisms for resolving regulatory conflicts will minimize uncertainty and reduce the likelihood of legal disputes. Enhancing regulatory clarity and certainty will foster a more favorable environment for innovation and competition in the EU digital market. EU judges must also address the deficiencies of the DMA through judicial review to mitigate the legislation's unintended repercussions.

References

1. Andriychuk, O. (2023). Do DMA obligations for gatekeepers create entitlements for business users? *Journal of Antitrust Enforcement*, 11(1), 123–132. <https://doi.org/10.1093/jaenfo/jnac034>
2. Bania, K. (2023). Fitting the Digital Markets Act in the existing legal framework: The myth of the “without prejudice” clause. *European Competition Journal*, 19(1), 116–149. <https://doi.org/10.1080/17441056.2022.2156730>
3. Bostoen, F. (2023). Understanding the Digital Markets Act. *The Antitrust Bulletin*, 68(2), 263–306. <https://doi.org/10.1177/0003603X231162998>
4. Cennamo, C., Kretschmer, T., Constantinides, P., Alaimo, C., & Santaló, J. (2023). Digital platforms regulation: An innovation-centric view of the EU's Digital Markets Act. *Journal of European Competition Law & Practice*, 14(1), 44–51. <https://doi.org/10.1093/jeclap/lpac043>
5. Colangelo, G. (2023). Antitrust unchained: The EU's case against self-preferencing. *GRUR International*, 72(6), 538–556. <https://doi.org/10.1093/grurint/ikad023>
6. Deutscher, E. (2022). Reshaping digital competition: The new platform regulations and the future of modern antitrust. *The Antitrust Bulletin*, 67(2), 302–340. <https://doi.org/10.1177/0003603X221082742>
7. Hornung, P. (2024). The ecosystem concept, the DMA, and section 19a GWB. *Journal of Antitrust Enforcement*, 12(3), 396–437. <https://doi.org/10.1093/jaenfo/jnad049>
8. Knapstad, T. (2023). Breakups of digital gatekeepers under the Digital Markets Act: Three strikes and you're out? *Journal of European Competition Law & Practice*, 14(7), 394–409. <https://doi.org/10.1093/jeclap/lpad035>

9. Lamadrid de Pablo, A., & Bayón Fernández N. (2021). Why the proposed DMA might be illegal under Article 114 TFEU, and how to fix it. *Journal of European Competition Law & Practice*, 12(7), 576–589. <https://doi.org/10.1093/jeclap/lpab059>
10. Monti, G. (2022). Taming digital monopolies: A comparative account of the evolution of antitrust and regulation in the European Union and the United States. *The Antitrust Bulletin*, 67(1), 40–68. <https://doi.org/10.1177/0003603X211066978>
11. Podszun, R. (2023) From competition law to platform regulation — regulatory choices for the Digital Markets Act. *Economics*, 17(1), Article 20220037. <https://doi.org/10.1515/econ-2022-0037>
12. Turner, S., & Tanczer, L. M. (2024). In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review*, 52, Article 105912. <https://doi.org/10.1016/j.clsr.2023.105912>

Information about the author:

Kolawole O. Afuwape — LL.M. (University of Dundee, Scotland, United Kingdom), LL.M. (Lagos State University, Nigeria), Lecturer, Jindal Global Law School, O.P. Jindal Global University, Sonipat, India.
afuwapekolawole@gmail.com
ORCID: <https://orcid.org/0009-0001-5686-230X>

Сведения об авторе:

Афувапе К. О. — магистр права (Университет Данди, Шотландия, Соединенное Королевство), магистр права (Государственный университет Лагоса, Нигерия), преподаватель, Глобальный университет им. О. П. Джиндала, Сонипат, Индия.
afuwapekolawole@gmail.com
ORCID: <https://orcid.org/0009-0001-5686-230X>

СТАТЬИ

БАЛАНС ИНТЕРЕСОВ ПОЛЬЗОВАТЕЛЕЙ, ИЗДАТЕЛЕЙ И РАЗРАБОТЧИКОВ ПРИ ЗАКРЫТИИ ВИДЕОИГР В СВЕТЕ НОВОЙ ЕВРОПЕЙСКОЙ ИНИЦИАТИВЫ

Д. В. Граф

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

Аннотация

Приобретая игру, пользователи полагают, что им будет обеспечен не ограниченный каким-либо сроком доступ к продукту, что не всегда соответствует реальности. Зачастую непрозрачный лицензионный характер отношений между издателями и пользователями оставляет последних в неуверенности относительно их прав и не гарантирует им стабильность доступа к игре, которая может быть в любой момент закрыта. Такой дисбаланс вызывает основания полагать действующее регулирование не вполне справедливым. Эмпирическую основу исследования составляют нормативно-правовые акты и пользовательские соглашения, регулирующие отношения между издателями и пользователями при закрытии игровых проектов. Особое внимание уделяется анализу европейской гражданской инициативы «Stop destroying videogames», призывающей обеспечить функциональность игр даже после прекращения их поддержки. Цель исследования — выявить конкретные способы разрешения конфликта интересов между издателями, разработчиками и пользователями в случае закрытия игры. Посредством анализа указанной инициативы, оценки ее достоинств и недостатков, системного сравнения с актами в сфере авторского права и защиты прав потребителей было установлено, что, несмотря на ограниченное посягательство на свободу договора и интеллектуальные права разработчиков и издателей, указанная инициатива способствует достижению эффективного баланса прав и интересов всех сторон. По результатам исследования автор приходит к выводу о справедливости наложения на издателей и разработчиков ряда обязанностей, среди которых, например, удаление технических средства защиты авторских прав, которые реализуются за счет подключения к серверам разработчика, дозволение частного хостинга серверов и изменение модели распространения игр, а также компенсация части затрат пользователей в случае закрытия игр в раннем доступе.

Ключевые слова

лицензионный договор, закрытие игр, пользовательские соглашения, европейская гражданская инициатива, видеоигры, авторское право

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имеет спонсорской поддержки.

Для цитирования

Граф, Д. В. (2024). Баланс интересов пользователей, издателей и разработчиков при закрытии видеоигр в свете новой европейской инициативы. *Цифровое право*, 5(2), 24–39. <https://doi.org/10.38044/2686-9136-2024-5-2-24-39>

Поступила: 22.04.2024, принята в печать: 31.05.2024, опубликована: 28.06.2024

ARTICLES

BALANCING THE INTERESTS OF USERS, PUBLISHERS AND DEVELOPERS IN CASES OF SHUTDOWN OF VIDEO GAMES: A NEW EUROPEAN INITIATIVE

Denis V. Graf

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

Abstract

When purchasing a game, users assume that they will have ongoing unlimited access to the product—a notion that does not always correspond to reality. The nature of the relationship between publishers, developers and users as expressed in opaque licensing documentation often leaves the latter uncertain about their rights and does not guarantee them stable access to the game, which can be revoked at any time. This imbalance gives grounds to view the current regulatory framework as not entirely fair. The present study is based on statutory acts and user agreements that govern the relationship between publishers and users in cases of shutdown of gaming projects. Particular attention is paid to the analysis of the European citizens' initiative "Stop destroying videogames," which calls for ensuring the functionality of games even after developer support has ceased. The aim of the study is to identify concrete methods for resolving the conflict of interests between publishers, developers, and users in the event of a game closure. Through an analysis of the aforementioned initiative, an evaluation of its merits and shortcomings, and a systematic comparison with statutory acts in the fields of copyright and consumer protection, it has been determined that, despite its limited restriction of the freedom of contract and the intellectual property rights of developers and publishers, the initiative contributes to achieving an effective balance of the rights and interests of all parties. Based on the study's findings, the author concludes that it is fair to impose a number of obligations on publishers and developers. These obligations include, for example, the removal of technical measures for copyright protection, which are implemented via connections to the developer's servers, the permission for private server hosting, and the alteration of the game distribution model, as well as compensating users for part of their expenses in the event of the closure of games in early access.

Keywords

license agreement, shutdown of games, User agreements, European Citizens' Initiative, video games, copyright

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Graf, D. V. (2024). Balancing the interests of users, publishers and developers in cases of shutdown of video games: A new European initiative. <i>Digital Law Journal</i> , 5(2), 24–39. https://doi.org/10.38044/2686-9136-2024-5-2-24-39

Submitted: 22 Apr. 2024, accepted: 31 May 2024, published: 28 June 2024

Введение

Традиционная модель распространения видеоигр, предполагавшая физическое тиражирование и неограниченный доступ пользователя при наличии соответствующего технического обеспечения, претерпела существенные изменения в условиях цифровизации. Распространение видеоигр на цифровых рынках, значительно ускоренное развитием глобальной сети Интернет (Harkai, 2022, p. 846), привело к трансформации самой природы видеоигры, рассматриваемой ныне не столько как продукт, сколько как услуга (Lehtonen et al., 2022, p. 564). Правовое положение пользователей стало менее стабильным, так как теперь для доступа к игре недостаточно одного лишь наличия диска с ее экземпляром, позволяющего запускать игру в течение неограниченного времени при наличии нужного оборудования, а зачастую требуется и постоянное подключение к сети Интернет и согласие с лицензионным соглашением пользователя (*EULA*), которое часто меняется и по которому издатели могут ограничивать доступ к игровому контенту или даже полностью лишать пользователя доступа к игре без объяснения причин. В контексте динамичного развития индустрии онлайн-игр, особенно в период пандемии *COVID-19*, отмеченный резким ростом пользовательской аудитории (King et al., 2020, p. 184), многие игровые проекты, не выдержав конкуренции, ликвидируются, что сопровождается прекращением функционирования серверов, вследствие чего доступ пользователей к приобретенной игре может быть затруднен или вовсе невозможен. Данное явление порождает негативную реакцию со стороны сообщества, инвестировавшего значительные временные и финансовые ресурсы в указанные игровые проекты.

Актуальность настоящего исследования обусловлена недавними случаями закрытия таких популярных проектов, как *The Crew*, лицензии на которую были отозваны у пользователей из-за трудностей с продлением лицензий на использование в игре различных элементов и необходимости освобождения серверов для новых проектов — *Battlefield 3* и *4*, поддержка которых была прекращена на довольно старых моделях игровых консолей *PS3* и *XBox 360*. Если для издателей это решение было предсказуемым и было обосновано среди прочего необходимостью снижения своих издержек на поддержание серверов теряющих свою популярность проектов, то среди пользователей это вызвало волну негодования, поскольку они потеряли доступ к купленным внутриигровым предметам, а в случае с *The Crew* — и вовсе доступ

к игре, так как она не предусматривала наличие режима одиночной игры без подключения к сети. Указанные события привели к появлению европейской гражданской инициативы «*Stop Destroying Videogames*»¹ (далее — европейская инициатива), направленной на призывы к издателям обеспечивать функциональность видеоигр даже после прекращения их официальной поддержки.

Целью настоящего исследования является выявление возможных механизмов разрешения конфликта интересов между издателями, разработчиками и пользователями, гарантирующих соблюдение прав всех сторон правоотношений, после закрытия игровых проектов.

Для достижения вышеуказанной цели поставлены следующие задачи:

1. Анализ правовой природы соглашений в игровой индустрии;
2. Анализ европейской инициативы, а также ряда правовых норм на предмет их применимости к рассматриваемым отношениям;
3. Рассмотрение недостатков и перспектив предлагаемого механизма;
4. Предложение авторских способов разрешения рассматриваемой проблемы.

Правовая природа соглашений в игровой индустрии

Интересующими нас субъектами в рамках данного исследования являются издатели, разработчики и пользователи. Рассмотрим природу отношений между ними.

Согласно общепринятой практике отношения между разработчиками и издателями регулируются лицензионным договором, иначе называемым договором на издание видеоигры. По такому договору разработчик игры обычно отвечает за создание игрового мира, механику, графику, звука и кода. Это творческий и технический процесс, включающий в себя проектирование, программирование и в большинстве случаев внутреннее тестирование, хотя окончательный контроль качества может разделяться с издателем. Издатель же в основном отвечает за коммерческую составляющую: он финансирует разработку, занимается продвижением игры, обеспечивает ее дистрибуцию через различные каналы (магазины, цифровые платформы). Отметим, впрочем, что не всегда игровые компании прибегают к помощи сторонних издателей, иногда и сам разработчик сочетает в себе обе роли. Пример — игра *Hellblade: Senua's Sacrifice*, где и разработчиком, и издателем выступает компания *Ninja Theory*.

Характер такого договора может варьироваться в зависимости от размера и опыта обеих сторон, а также стадии разработки проекта, однако все включают общие элементы, которые мы рассмотрим на примере некоторых реальных соглашений².

- **Права на интеллектуальную собственность.** Данный раздел включает в себя распределение прав на игру и входящие в нее результаты интеллектуальной деятельности (например, музыку, графические материалы и т.д.). В основном предусматривается, что такие права принадлежат разработчику и предоставляются по лицензии издателю на определенный срок или без ограничения во времени с указанием конкретных территорий и платформ

¹ European Citizens' Initiative. (2024). *Stop Destroying Videogames*. European Commission. https://citizens-initiative.europa.eu/initiatives/details/2024/000007_en

² Мы рассмотрим соглашение между *Publ'g License Agreement between Double Fine Prod's, Inc. & Fig Publ'g, Inc., U.S. Sec. & Exch. Comm'n*, https://www.sec.gov/Archives/edgar/data/1658966/000121390016017352/f1u093016ex6ii_figpublishing.htm (Aug. 5, 2016) (далее — соглашение Fig) и стандартное соглашение издателя *Raw Fury AB* с разработчиками *Dev. & Publ'g Agreement*, <https://rawfury.com/developer-resources/> (Feb. 22, 2022) (далее — соглашение Raw Fury).

распространения. Так, разд. 3 соглашения *Raw Fury* содержит положение о том, что издателю предоставляются по лицензии исключительные права «публиковать, воспроизводить, продвигать, рекламировать, экспортировать, импортировать, сублицензировать, переводить, распространять, демонстрировать, продавать, сдавать в аренду и иным образом использовать игру»; впрочем, разработчик также может использовать ряд обозначенных прав в целях продвижения игры или иных обоюдно выгодных целях. Схожие положения содержатся и в соглашении *Fig* (разд. 1.1), однако по нему издателю предоставляется неисключительная лицензия. Важно также отметить, что отдельные игры могут использовать чужие результаты интеллектуальной деятельности. Так, например, условия использования игры *Just Dance* содержат положение³, согласно которому пользователь признает, «что все материалы в Сервисах, включая дизайн, графику, текст, звуки, изображения, программное обеспечение и другие файлы, являются собственностью *UBISOFT*, ее материнской компании или ее лицензиаров...». Обычно за получение лицензий на результаты интеллектуальной деятельности третьих лиц отвечает разработчик.

- **Финансирование.** В этом разделе содержатся условия финансирования проекта со стороны издателя, включая размеры авансов, промежуточных выплат и роялти после релиза игры. Доходы могут распределяться между разработчиком и издателем либо в процентном соотношении (как это сделано в соглашении *Raw Fury*: документ указывает, что доля издателя составляет 50%), либо в конкретных денежных суммах (как в соглашении *Fig*: разд. 6.3 предусматривает правила их расчета).
- **Процесс разработки.** В этом разделе содержится регламентация сроков разработки, этапов создания игры, утверждения ключевых решений по дизайну и геймплею. Если некоторые соглашения дают большую свободу разработчику, ограничивая его лишь необходимостью сдать готовый продукт к обозначенному сроку (см., например, разд. 10 соглашения *Raw Fury*), то другие соглашения могут включать требование сдачи промежуточной отчетности (см., например, разд. 3 соглашения *Fig*).
- **Маркетинг и дистрибуция.** В этой части предусматриваются стратегии продвижения игры, каналы дистрибуции (цифровые магазины, физические носители) (см., например, разд. 1.1.2 соглашения *Fig*, разд. 1 соглашения *Raw Fury*), а также распределение затрат и прибыли от продаж. Несмотря на то что в основном указанная сфера находится в ведении издателя, стороны вольны согласовывать определенные характеристики данного раздела (например, ограничить список платформ для рекламы по воле разработчика).
- **Ограничения.** Иногда могут встречаться положения, ограничивающие разработчика в возможности создания схожей игры. Так, соглашение *Raw Fury* гласит, что разработчик не должен разрабатывать игру, настолько похожую на ту, которая является предметом этого соглашения, что существует риск ввести потребителей в заблуждение, или игру, использующую тот же исходный код, но с незначительными эстетическими изменениями, в течение года после выхода игры, выступающей предметом названного соглашения.
- **Расторжение договора.** Данный раздел содержит основания для расторжения договора, а также его последствия. Особо обратим внимание на то, что в основном в рассматриваемых соглашениях содержится положение, обязывающее разработчиков возмещать затраты издателя на разработку и маркетинг игры в случае досрочного расторжения договора по вине разработчика (см., например, разд. 22 соглашения *Raw Fury*: «При существенном нарушении условий соглашения разработчиком издатель вправе потребовать от него воз-

³ *Ubisoft Terms of use*, <https://justdancelive.com/ubisoft-terms-of-use/> (Jan. 12, 2016).

врата первоначального аванса и любых дополнительных выплат (а также другого финансирования)»).

Несмотря на то что договор на издание игры не регулирует отношения с конечными пользователями, его условия непосредственно влияют на возможность защиты их прав. Очевидно, что издатель не сможет передать пользователям больше прав, чем есть у него, и не сможет обеспечить должную защиту пользователя при закрытии серверов: банальным препятствием станут лицензии на результаты интеллектуальной деятельности третьих лиц.

Что касается отношений между издателями и пользователями, то они также базируются на лицензионном договоре, который, впрочем, содержит другой перечень прав, обязанностей и ограничений. Этот вид договоров дает возможность правообладателям ограничивать права пользователей не только на основании законодательных норм авторского права, но и в рамках договорных отношений (Mezei & Harkai, 2022, p. 2).

В отличие от договора на издание видеоигры, условия которого могут адаптироваться к конкретным обстоятельствам и обсуждаться сторонами, пользовательское соглашение представляет собой договор присоединения, предлагаемый издателем игрокам при установке или запуске игры. Как верно отмечается некоторыми исследователями, пользовательское соглашение имеет смешанную природу и сочетает в себе «элементы договора оказания услуг, лицензионного договора о неисключительном праве использования видеоматериалов и программ, а также согласия на обработку персональных данных» (Andrianova & Vlasenko, 2020, p. 27).

Пользовательское соглашение, как правило, содержит следующие важные моменты:

- **Предоставление лицензии.** Пользовательское соглашение предоставляет игроку неисключительную лицензию на использование программного обеспечения и иных компонентов игры (в том числе внутриигровых предметов), а не исключительное право на них. Рассмотрим примеры:
 - *Условия оказания услуг Riot Games*⁴: «Вы (пользователь) получаете лицензию только на доступ к Виртуальному контенту. Вы не приобретаете права собственности на какой-либо разблокированный вами Виртуальный контент»;
 - *Лицензионное соглашение с конечным пользователем Blizzard*⁵: «Использование вами (пользователем) Платформы осуществляется по лицензии, а не продается, и вы тем самым подтверждаете, что никакие права собственности в отношении Платформы или Игр не передаются и не уступаются и настоящее Соглашение не должно толковаться как продажа каких-либо прав»;
 - *Лицензионное соглашение с конечным пользователем Ubisoft*⁶: «Данная Лицензия не предоставляет Вам (пользователю) право собственности на Продукт и не должна рассматриваться как продажа каких-либо прав на Продукт»;
 - *Соглашение подписчика Steam*⁷: «Настоящим передается право пользования Контентом и Услугами, а не какие-либо иные вещные права. Передаваемое право не порождает никакого титула или права собственности на Контент и Услуги».

⁴ Условия оказания услуг Riot Games, <https://www.riotgames.com/ru/terms-of-service-RU> (Sept., 15, 2015).

⁵ End User License Agreement, <https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement> (Mar. 21, 2024).

⁶ Лицензионное соглашение с конечным пользователем, Ubisoft, <https://legal.ubi.com/eula/ru-RU> (last visited Mar. 14, 2024).

⁷ Соглашение подписчика Steam, Steam, https://store.steampowered.com/subscriber_agreement/?l=russian (last visited Mar. 14, 2024).

- **Ограничения ответственности издателя за ущерб, причиненный игроку в результате использования игры.** Это может включать в себя исключение ответственности за косвенные убытки, убытки, связанные с потерей данных, вред, причиненный виртуальному имуществу, и т.д. Рассмотрим примеры.
 - *Условия оказания услуг Riot Games:* «Riot Games никоим образом не несет ответственности за уничтожение, удаление, изменение, повреждение, взлом Виртуального контента или любой иной ущерб или вред любого рода, причиненный Виртуальному контенту, включая удаление Виртуального контента при удалении или истечении срока действия Вашей учетной записи, а также в результате разумных изменений, вносимых нами в Сервисы Riot»;
 - *Соглашение подписчика Steam:* «в максимально допустимой соответствующим законом степени Valve [компания, предлагающая онлайн-службу Steam, где распространяются игры]... не несет ответственности за убытки, ставшие следствием использования или невозможности использования службы Steam, вашего аккаунта, ваших подписок и контента и услуг, в том числе потерю нематериальных активов».
- **Прекращение действия соглашения.** Положения данного раздела в большей степени, чем остальные, служат интересам издателя, поскольку позволяют прекратить доступ пользователя к игре или аккаунту по самым разным причинам; при этом, как было отмечено выше, у пользователя в таких случаях не возникнет право требовать соответствующего возмещения. Рассмотрим примеры.
 - *Лицензионное соглашение с конечным пользователем Blizzard:* «Blizzard оставляет за собой право расторгнуть настоящее Соглашение в любое время по любой причине или без таковой, с уведомлением вас или без него»;
 - *Лицензионное соглашение с конечным пользователем Ubisoft:* «Прекращение действия данного Соглашения компанией UBISOFT вступит в силу после (a) уведомления Вас или (b) закрытия Вашего Аккаунта (при наличии такового) либо (c) в момент принятия решения компанией UBISOFT о прекращении действия предложения и (или) поддержки Продукта»;
 - *Условия оказания услуг Riot Games:* «Мы можем удалить Вашу учетную запись или приостановить ее действие, если мы обоснованно установим, что: ...это отвечало бы интересам нашего сообщества или Сервисов Riot...; мы прекратили предоставлять Сервисы Riot в Вашем регионе...»

Подводя итог данному разделу, отметим, что ключевое различие между издательским и пользовательским соглашениями заключается в характере отношений и в гибкости договорных условий. Издательское соглашение — это договор между равноправными (в теории) сторонами, предполагающий переговоры и компромиссы. Пользовательское соглашение представляет собой договор присоединения, когда игрок принимает условия, предложенные издателем, или отказывается от игры; при этом такие условия не всегда могут в полной мере учитывать интересы пользователя, а их пересмотр возможен лишь в исключительных случаях, когда они явно противоречат нормам законодательства.

Впрочем, очевидно, что оба указанных вида соглашений являются проявлением принципа свободы договора, поскольку стороны (или как минимум одна из них) могут выбирать условия, на которых они будут предоставлять доступ к игре. В связи с этим перейдем к анализу европейской инициативы и рассмотрим в том числе вопрос о ее соотношении с условиями данных соглашений.

Ключевые положения европейской инициативы

Как следует из текста инициативы, ее целью является «требование от издателей, которые продают или передают по лицензии видеоигры потребителям в Европейском союзе... поддерживать указанные видеоигры в функциональном состоянии. В частности, инициатива направлена на предотвращение удаленного отключения видеоигр издателями, прежде чем будут предоставлены разумные средства для продолжения функционирования указанных видеоигр без участия издателя». Связаны такие требования с обозначенными во введении изменениями видеоигры. Видеоигра представляет собой сложный мультимедийный продукт, который включает несколько результатов интеллектуальной деятельности, охраняемых авторскими правами: это и непосредственно код, и музыкальное сопровождение, и графические материалы, и т.д. (Rozhkova, 2020, p. 7). Если ранее все такие данные содержались в физическом экземпляре пользователя, то сегодня частой практикой стало хранение части данных игры на серверах. Соответственно, игра включает в себя клиентскую часть⁸ (ту часть файлов, которая устанавливается на устройство пользователя) и серверную часть. При отключении серверов игрок лишается возможности использования всего или части функционала игры.

Важно отметить, что авторы европейской инициативы не требуют от издателей передачи им всех прав на игру, включая интеллектуальные права и договорные права (например, права на монетизацию). Они ссылаются прежде всего на положения ст. 17 Хартии Европейского союза об основных правах, гласящей, что «никто не может быть лишен своего имущества, кроме как в общественных интересах и в случаях и на условиях, предусмотренных законом, при условии своевременной выплаты справедливой компенсации за его утрату»⁹, а также на статьи Договора о функционировании Европейского союза, содержащего общие положения о необходимости защиты прав потребителей. Такая коммодификация видеоигр, проявляющаяся в их превращении в значимый объект рыночного оборота, сопровождается парадоксальным явлением. Стремление к максимизации прибыли, обусловленное интенсивной конкуренцией и высоким потребительским спросом, стимулирует ускорение цикла разработки и выпуск новых продуктов вкупе с прекращением поддержки и закрытием серверов после относительно короткого периода эксплуатации. Это демонстрирует конфликт между логикой рыночной оптимизации и потребительским ожиданием долгосрочного владения и пользования цифровым продуктом, аналогично владению материальными благами и порождает определенный конфликт интересов. С точки зрения права здесь встает вопрос о том, в какой степени нетипичные имущественные права, передаваемые пользователям, могут рассматриваться как имущество и, соответственно, насколько к ним будут применимы гарантии имущественных прав.

Прежде чем выявлять достоинства и недостатки европейской инициативы и ее эффективность в разрешении указанного конфликта, стоит более подробно рассмотреть вопрос о применимости гарантий ст. 17 Хартии Европейского союза об основных правах к играм и о том, насколько эффективно могут защищать права пользователя при закрытии серверов положения нормативно-правовых актов, посвященных, в частности, защите прав потребителей.

⁸ Такой термин упоминается, например, в п. 5.7. Лицензионного соглашения с конечным пользователем «Леста Игры»: *Лицензионное соглашение с конечным пользователем*, Lesta Games, <https://legal.lesta.ru/eula/> (last visited Sep. 14, 2023).

⁹ Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

Применение правовых норм к отношениям, возникающим при закрытии серверов

Говоря о применимости гарантий ст. 17 Хартии Европейского союза об основных правах к играм, отметим, что данный вопрос в несколько иной формулировке уже рассматривался многими учеными, в том числе J. Fairfield (2005), М.А. Рожковой (Rozhkova, 2020) и иными¹⁰. Более того, такой подход находит свое воплощение в ряде зарубежных порядков¹¹: суды иногда признают за игроками квазиимущественные права на виртуальные предметы. Впрочем, случаи применения данной концепции ограничиваются уголовно-правовой сферой.

На наш взгляд, распространение гарантий имущественных прав на игры затруднено тем фактом, что гражданско-правовые отношения по поводу пользования игрой и виртуальным имуществом не являются абсолютными, поскольку правам одного игрока противопоставлены обязанности лишь ограниченного круга лиц: правообладателя игры и таких же других игроков, которые получили доступ к игре. Для защиты прав пользователей здесь понадобятся скорее иные особые механизмы вроде стандартизации договорных условий, контроля за ними и т. д.

Помимо этого, есть и иные причины, почему распространение гарантий имущественных прав на игры, в частности вещно-правовых гарантий, едва ли является возможным. Во-первых, вещное право, в частности право собственности, регулирует отношения, связанные с владением, пользованием и распоряжением материальными, индивидуально-определенными вещами. В случае онлайн-игры отсутствует как материальность (материален лишь диск, на который игра может быть записана), так и индивидуальная определенность. Именно по этой причине игры как нематериальные, сложные объекты, включающие в себя несколько результатов интеллектуальной деятельности, будут подпадать под нормы об исключительном праве в сфере интеллектуальной собственности, которому присуще большее, чем иным имущественным правам, количество ограничений в отношении их границ и содержания, а также сроков действия. Во-вторых, применение вещно-правовой концепции затруднено вследствие чрезмерно большого числа игроков, а также потому, что это может неблагоприятно отразиться на развитии индустрии: это может повлечь ответственность разработчиков или издателей за внесение изменений в виртуальный мир (Saveliev, 2014, p. 140), а при закрытии утративших актуальность проектов — обязанность возмещения пользователям ущерба, причиненного уничтожением их имущества (Medvedev, 2018, p. 148).

Переходя к правовым актам, посвященным защите прав потребителей, они в данном случае показывают свою неэффективность. Так, ст. 8 Директивы ЕС о некоторых аспектах, касающихся контрактов на поставку цифрового контента и цифровых услуг предусматривает требование соответствия продукта условиям договора, что, по мнению некоторых исследователей, привело бы к тому, что «для соблюдения объективных требований к соответствию компьютерная игра должна была бы соответствовать своей пробной версии» (Wiśniewska & Pałka, 2023, p. 396), если она предоставляется (пробная версия является предварительной (как

¹⁰ См., в частности Lastowka et al. (2004), S. H. Abramovich (2007).

¹¹ В качестве примера здесь можно привести несколько знаменитых судебных решений. Во-первых, это решение Верховного суда Нидерландов по делу HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (Neth.), где игрока под угрозой насилия и убийства заставили «уронить» в игре две вещи — там суд распространил на внутриигровые предметы положения об имуществе. Во-вторых, это дело *Li Hongchen v. Beijing Arctic Ice Technology Development Co.* (Chin.) (приводится по Fairfield (2005, p. 1084)), в котором у игрока хакером были украдены внутриигровые предметы — суд признал их имуществом и обязал их вернуть в инвентарь игрока.

правило, бесплатной и ограниченной в своем функционале) версией игры, которая создается с целью дать представление пользователям о полной (иногда еще готовящейся) версии игры; при этом зачастую некоторые элементы из пробной версии не попадают в финальную версию игры). Кроме того, стоит учитывать, что положения пользовательских соглашений зачастую содержат в себе дисклеймеры, т.е. отказы от каких-либо претензий, связанных с характеристиками услуги: например, разъясняя, что платформа, учетные записи и игры предлагаются на условиях «как есть» и «как доступно», без каких-либо гарантий, пользователей информируют о том, что они принимают на себя риски, присущие их взаимодействию с платформой и связанными с ней играми (Lau, 2024, p. 83). Отход от положений этих соглашений возможен в исключительных случаях, например, когда лицензионное соглашение нарушает права потребителей или их разумные ожидания на основании предполагаемого несоответствия цифрового контента *явно сделанным при продаже заверениям* (Oprysk, 2021, p. 951). Например, согласно ответу Департамента культуры, СМИ и спорта Великобритании, «издатели должны предоставлять четкую информацию и обеспечивать постоянный доступ к играм в случае их продажи, при условии, что в них можно будет играть бесконечно»¹². Это правило включено и в некоторые пользовательские соглашения: например, согласно условиям оказания услуг *Riot Games*, названная компания не ограничивает свою ответственность за любую гарантию, предоставленную игроку.

Несмотря на потенциальную возможность оспаривания положений пользовательских соглашений, ограничивающих ответственность разработчиков и издателей видеоигр, прецеденты судебного признания недействительности таких оговорок в сфере видеоигр на настоящий момент отсутствуют. Стандартные формулировки, широко распространенные в индустрии, а также использование визуальных средств (например, выделение ключевых положений заглавными буквами), направленных на обеспечение презумпции осведомленности пользователя и усиление доказуемости его согласия с условиями пользовательского соглашения пока что показывают свою эффективность.

Говоря о положениях актов в сфере авторского права, отметим, что в ЕС отсутствуют акты, которые эффективно бы разрешали данный вопрос. В связи с этим в качестве примера удачного регулирования обратимся к положению акта США. Согласно п. 17 разд. 201.40 ч. 201 Свода федеральных нормативных актов, запрет на обход технологических мер, контролирующих доступ к произведениям, защищенным авторским правом, не распространяется на пользователей «полных видеоигр [т.е. таких, в которые пользователи могут играть без доступа к защищенному авторским правом контенту, хранящемуся или ранее хранившемуся на внешнем компьютерном сервере, или без его воспроизведения]... которые были законно приобретены... когда владелец авторских прав или его уполномоченный представитель прекратил предоставлять доступ к внешнему компьютерному серверу»¹³. При этом разрешаются: «модификации компьютерной программы с целью восстановления доступа к игре для персонального, локального игрового процесса на персональном компьютере или игровой приставке» и «с целью обеспечить сохранение игры в пригодной для воспроизведения форме соответствующей библиотекой, архивом или музеем».

Стоит заметить, что упомянутый авторско-правовой механизм действительно довольно эффективно решает проблему отключения серверов одиночных игр, однако

¹² Petition to U.K. Parliament, “Require Mandatory Labeling of AI-Generated Content,” Petition No. 659071 (May 2024), <https://petition.parliament.uk/archived/petitions/659071>

¹³ 37 C.F.R. § 201.40 (2024), <https://www.copyright.gov/title37/201/37cfr201-40.html>

не в полной мере отвечает интересам пользователей при прекращении работы серверов многопользовательских онлайн-игр. Во-первых, нередки случаи, когда ряд файлов хранится не на устройствах пользователей, а на серверах издателей, т.е. после закрытия пользователи фактически не будут иметь возможности как-либо адаптировать программу. Во-вторых, данный механизм, как это следует из документа Бюро авторского права США, не позволяет восстанавливать доступ к «многопользовательской онлайн-игре в значительной степени из-за того, что... неясно, как можно было бы предоставить средства обхода технических средств защиты для нескольких пользователей, чтобы облегчить альтернативный способ поиска матчей»¹⁴, не нарушая вместе с тем разд. 1201 Закона об авторском праве в цифровую эпоху США¹⁵, предусматривающий запрет на незаконный оборот продуктов или устройств, которые обходят технологические меры, используемые владельцами авторских прав для ограничения доступа к своим произведениям. В-третьих, пользователи не заинтересованы в самостоятельной адаптации программы и не всегда обладают нужными для этого навыками, в связи с чем они, скорее, захотят получить уже готовый к использованию продукт.

Анализ европейской инициативы

Учитывая вышесказанное, но не ограничиваясь этим, отметим следующие черты рассматриваемой нами европейской гражданской инициативы.

Заметно, что она ограничивает свободу договора. Как было рассмотрено выше, пользовательское соглашение предоставляет пользователю лицензию, т.е. разрешение, на использование игры. Природа такого соглашения подразумевает временный характер доступа к игре. Это вытекает в том числе и из названия некоторых пользовательских соглашений, именуемых «условия предоставления услуг», т.е. как некий ограниченный во времени комплекс действий в виде предоставления доступа к продукту. Кроме того, в пользовательском соглашении предусмотрено право издателя прекращать доступ к онлайн-игре по различным причинам без выплаты каких-либо компенсаций (выплата справедливой компенсации упоминается в Хартии Европейского союза, на которую ссылаются авторы европейской инициативы). Необходимость предоставлять неограниченный доступ к продукту после принятия решения о закрытии проекта идет вразрез с обозначенными в пользовательском соглашении полномочиями издателя. Следовательно, предлагаемые идеи могут некоторыми справедливо считаться значительно ограничивающими договорную свободу.

Кроме того, европейская инициатива содержит ряд недостатков. Первым существенным упущением недостатком является отсутствие конкретных критериев определения «функционального состояния» игры, что является критически важным. Без такого четкого определения осложняется правовое регулирование ситуаций, связанных с утратой совместимости игры с пользовательским оборудованием спустя длительный период после прекращения функционирования серверов. Из текста европейской инициативы неясно, какую степень «функциональности» должны обеспечивать правообладатели; в ней не установлен временной интервал, в течение которого должна поддерживаться функциональность игры.

¹⁴ U.S. Copyright Office, *Section 1201 Rulemaking: Register's Recommendation* (2024), https://www.copyright.gov/1201/2024/2024_Section_1201_Registers_Recommendation.pdf.

¹⁵ 17 U.S.C. § 1201.

Вторым недостатком является неопределенность распределения ответственности за обеспечение функциональности игры. Текст европейской инициативы не упоминает лицо, которое должно отвечать за приведение игры в функциональное состояние и, что тоже важно, источник компенсации этому лицу расходов на данные действия. Подобные пробелы могут вызвать существенные сложности при заключении разработчиками договоров с издателями; особенно это касается небольших разработчиков, и без того сталкивающихся с многочисленными трудностями в своей деятельности (Limpach, 2020, p. 7).

Третьим недостатком выступает тот факт, что предлагаемые положения могут ограничить возможность реализации разработчиками права на защиту своей деловой репутации. В частности, если закрытие игрового проекта вызвано не сугубо финансовыми причинами, а личными мотивами разработчика, который спустя какое-то время счел свой продукт недостаточно качественным или противоречащим его воззрениям, то обязанность по обеспечению вечной функциональности такого продукта может нанести ему существенный репутационный ущерб на протяжении длительного периода времени.

Четвертый недостаток — потенциальные маркетинговые ограничения. Так, например, игра *FIFA* реализуется по модели, которая предполагает издание новой версии каждый год с закрытием серверов более старых версий спустя какое-то время. При вечном функционировании каждой версии игры издатели будут нести значительные убытки, поскольку пользователи перестанут покупать новый продукт, довольствуясь тем, что у них уже есть.

Считаем, что некоторые обозначенные недостатки действительно заслуживают внимания и могут быть нейтрализованы при надлежащей реализации выдвигаемых европейской инициативой предложений.

Другие же доводы могут быть опровергнуты. В частности, аргумент о маркетинговых ограничениях не обладает достаточной силой, учитывая, что потребители могут отказаться от покупки новой игры по собственной воле, не обусловленной наличием или отсутствием у них экземпляров других версий игры. Кроме того, модель, при которой игра выпускалась бы единоразово и сопровождалась регулярными обновлениями, предоставила бы более широкие возможности для взаимодействия с пользователями (Dubois & Weststar, 2022, p. 2342) и позволила бы экономить время и средства, вкладываемые в производство отдельных игр (сюда включаются и разработка, и расходы на создание экземпляров). Возможный ущерб репутации также не является существенным, поскольку любое творческое произведение, включая видеоигру, имеет право на существование, и его ценность определяется субъективным восприятием.

На наш взгляд, рамочный характер европейской инициативы может являться в данном случае преимуществом. Учитывая тот факт, что она представляет собой лишь идею, решение об имплементации которой (и способах имплементации) в дальнейшем будут принимать соответствующие органы, законодатели смогут самостоятельно разработать эффективные механизмы, позволяющие соблюсти баланс интересов пользователей, издателей и разработчиков. Скорее всего, это потребует изобретения новых правовых конструкций, так как существующие ныне правовые положения едва ли могут быть в полной мере применимы к рассматриваемой проблеме.

Способы решения

С учетом вышеизложенных соображений мы предлагаем следующие рекомендации по реализации положений европейской инициативы.

Прежде всего разработка дополнительного программного кода для реализации, например, механики ботов (персонажей, управляемых автоматизированными программами) для восполнения аудитории после прекращения работы серверов и утраты игрой популярности, была бы нецелесообразной и выходила бы за рамки понятия «функциональности» видеоигры. Настолько же чрезмерной была бы и обязанность обеспечивать совместимость игры с устройствами пользователей в течение неограниченного времени. Некоторые исследователи рассматривают функциональность игры (или «играбельность») как обеспечение доступности игры на ее оригинальной платформе в соответствии с оригинальным игровым опытом (Newman, 2018, p. 264). И действительно, поскольку в настоящей статье сохранение функциональности игры рассматривается не с позиций необходимости защиты культурного наследия, что, вероятно, предполагало бы ее доступность для будущих поколений в течение долгого срока, подобно экспонатам в музее, а с позиции соблюдения интересов прав пользователей, на наш взгляд, предполагаемые обязанности по обеспечению совместимости должны ограничиваться соблюдением игрой характеристик, заявленных в ее последнем на момент закрытия серверов обновлении, с учетом указанных в источниках издателя и разработчика системных требований.

Кроме того, стоит отказаться и от идеи предоставления разработчиками исходного кода, в том числе потому, что он зачастую может рассматриваться как коммерческая тайна (Harkai, 2022, p. 850).

Переходя к конкретным предложениям, отметим, что, во-первых, потребуется внесение изменений в соглашения между издателями и разработчиками. На наш взгляд, реализация европейской инициативы потребует пересмотра нескольких разделов соглашения на издание игры, в частности разделов о финансировании (в случае если приведение игры в функциональное состояние потребует дополнительных усилий), о расторжении договора (будет необходимо уточнить момент прекращения обязательств сторон), об интеллектуальных правах (в случаях, когда специфика игры предполагает необходимость заключения лицензионных соглашений с третьими лицами).

Во-вторых, на наш взгляд, было бы целесообразным внести изменения в правовые акты с целью возложения на издателя и разработчика обязанности исправить игру после прекращения ее поддержки, чтобы удалить технические средства защиты авторских прав, которые реализуются за счет подключения к серверам разработчика, и допустить частный хостинг или, если соответствующие серверы не используются компаниями для других нужд, аренду этих серверов пользователями. Так было сделано, например, разработчиками игры *Knockout City*, которые выпустили ее в виде отдельного исполняемого файла для *Windows* с поддержкой частных серверов¹⁶. При этом важно, чтобы после закрытия серверов и передачи игры в своеобразное

¹⁶ Это позволяет игрокам использовать многопользовательский режим даже после отключения серверов на стороне разработчика, так как пользователи сами смогут запускать небольшие сервера, рассчитанные на ограниченное число людей на своих частных компьютерах. Впрочем, недостатками такого решения, по словам самого разработчика, является то, что авторам пришлось удалить все лицензированные ПО и косметические предметы, а также то, что у них был лишь один шанс выпустить рабочую версию программы, так как дальнейшая поддержка не подразумевается.

администрирование сообществу степень вовлеченности игроков и, соответственно, обеспечение их положительного опыта оставались за рамками обязательств разработчиков и издателей.

В отношении распределения ответственности за обеспечение функциональности игры оптимальным решением, по нашему мнению, было бы ее возложение на разработчика как на более компетентное лицо с учетом обязанности издателя компенсации понесенных затрат на модификацию игры для сохранения ее функциональности в случаях, когда прекращение поддержки игры вызвано действиями или решением издателя. Это потребует внесения изменений в соглашения между разработчиками и издателями. В то же время пользователям, если у них возникнет необходимость принудить разработчика к обеспечению функциональности, было бы целесообразно дать право обращаться к нему через издателя как своеобразного посредника в отношениях между разработчиками и пользователями.

В-третьих, в некоторых случаях потребуется корректировка модели предоставления доступа к игре, в частности отмена платных подписок с ограниченным сроком действия. Для соблюдения интересов издателя может быть предложено предоставление пользователям возможности приобретения не ограниченной сроком лицензии по повышенной цене для получения неограниченного доступа к игровым файлам; при этом отказ от такой покупки будет влечь за собой утрату права требования восстановления доступа.

В-четвертых, в случае прекращения поддержки игры, находившейся на стадии раннего доступа, целесообразно предусмотреть возврат пользователям части ранее уплаченных денежных средств. На наш взгляд, ответственное за выплату такой компенсации лицо должно определяться в издательском соглашении в зависимости от воли сторон, а размер соответствующего возмещения должен определяться с учетом степени реализации функций, заявленных на этапе раннего доступа, продолжительности периода раннего доступа и т.д.

Кроме того, издателям следует делать упор на информирование пользователей о характере правоотношений при покупке игры и о том, что серверы игры могут быть потенциально отключены. Так, недавний закон штата Калифорния обязал издателей уведомлять игроков, что они приобретают права по лицензии, т.е. доступ к купленному контенту может быть заблокирован в любое время¹⁷.

Определенно, все эти механизмы потребуют готовности к сотрудничеству со стороны разработчиков и издателей, поскольку попытки пользователей самостоятельно обеспечить функциональность игры нередко приводят к судебным разбирательствам, связанным с незаконным копированием и распространением игры¹⁸. Потенциальные правонарушения также могут быть связаны с созданием и использованием эмуляторов (Lee, 2018, p. 104) — программного обеспечения или устройств, имитирующих функциональность игровой системы.

Отметим, что для эффективной реализации положений инициативы потребуется также изменение правоприменительной практики. На сегодняшний день зарубежные суды нередко отказывают игрокам в удовлетворении требований, вытекающих из отношений по пользованию игровыми сервисами, на основании согласия игрока с правилами пользовательского соглашения¹⁹. Считаем, что стоит чаще рассматривать лицензионный договор с точки зрения его справедливости и добросовестности (как это было сделано, например, в кейсе *Bragg v.*

¹⁷ Cal. Bus. & Prof. Code § 17500.6 (2024).

¹⁸ *Atlas Co., Ltd. v. John Doe*, No. 1:21-cv-11102, (S.D.N.Y. 2022).

¹⁹ Можно упомянуть дело *Reynolds v. A Thinking Ape Entertainment Ltd.*, 2021 BCCRT 281 (Can.), где суд отказал в удовлетворении требований на том основании, что истица согласилась с «Правилами оказания услуг» данной игры, а они предусматривали возможность блокировки по любой причине.

*Linden Research, Inc.*²⁰, где суд не признал силу за несколькими положениями лицензионного соглашения²¹).

Заключение

Рассмотренная европейская гражданская инициатива является катализатором разрешения уже долгое время существующего между издателями, разработчиками и игроками конфликта. Несмотря на отсутствие в ней конкретики, кажущееся посягательство на интеллектуальные права разработчиков и издателей и свободу договора, она может привести к положительным изменениям, которые позволили бы соблюсти интересы всех сторон.

Дефицит эффективных правовых механизмов в действующих ныне правовых нормах, посвященных защите прав потребителей, и авторском праве, необходимых для реализации предложений, содержащихся в рассматриваемой инициативе, диктует необходимость расширения круга обязанностей издателей и разработчиков видеоигр. Предлагается законодательно закрепить обязанность по удалению технических средств защиты авторских прав, привязанных к серверам разработчиков, обеспечение возможности частного хостинга игрового ПО, изменение модели доступа к игре, а также компенсацию части затрат пользователей в случае игр, выпущенных в режиме раннего доступа. Необходимо также отметить важность изменения правоприменительной практики, с целью обеспечения эффективного рассмотрения споров в сфере видеоигр и снижения доминирующей роли пользовательских соглашений в регулировании отношений между пользователями и разработчиками / издателями.

Список литературы / References:

1. Abramovitch, S. H. (2007). Virtual property, real law: The regulation of property in video games. *Canadian Journal of Law and Technology*, 6(2), Article 2.
2. Andrianova, M. A., & Vlasenko, E. V. (2020). Riski provajdera, svyazannye s neopredelennost'yu pravovoj prirody pol'zovatel'skih soglashenij onlajn-igr [Provider risks connected with uncertainty in the legal nature of online games' terms of use]. *Digital Law Journal*, 1(3), 21–39. <https://doi.org/10.38044/2686-9136-2020-1-3-21-39>
3. Dubois, L.-E., & Weststar, J. (2022). Games-as-a-service: Conflicted identities on the new front-line of video game development. *New Media & Society*, 24(10), 2332–2353. <https://doi.org/10.1177/1461444821995815>
4. Fairfield, J. (2005). Virtual Property. *Boston University Law Review*, 85, 1047–1102.
5. Harkai, I. (2022). Preservation of video games and their role as cultural heritage. *Journal of Intellectual Property Law & Practice*, 17(10), 844–856. <https://doi.org/10.1093/jiplp/jpac090>
6. King, D. L., Delfabbro, P. H., Billieux, J., & Potenza, M. N. (2020). Problematic online gaming and the COVID-19 pandemic. *Journal of Behavioral Addictions*, 9(2), 184–186. <https://doi.org/10.1556/2006.2020.00016>
7. Lastowka, F. G. G., & Hunter, D. (2004). The laws of the virtual worlds. *California Law Review*, 92(1), 1–74.

²⁰ *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593 (E.D. Pa. 2007).

²¹ В данном деле пользователь нарушил пользовательское соглашение, за что его аккаунт был заблокирован. Ключевым вопросом стал выбор компетентного суда, в частности, исполнимость имеющейся в соглашении арбитражной оговорки. Суд решил, что арбитражная оговорка была неисполнимой, так как соглашение разбирательство в арбитраже было неоправданно затратным для пользователя, а он в свою очередь не имел каких-либо альтернатив (например, он не мог отказаться от пользования данной игрой и выбрать другую с более выгодными положениями в силу ее уникальности на рынке).

8. Lau, P. L. (2024). Disrupting MMORPGs gaming: Exploring and renegotiating end-user license agreements in the Metaverse. *International Journal of Commerce and Contracting*, 8(1–2), 65–87. <https://doi.org/10.1177/20555636241246188>
9. Lee, Y. H. (2018). Making videogame history: Videogame preservation and copyright law. *Interactive Entertainment Law Review*, 1(2), 103–108. <https://doi.org/10.4337/ielr.2018.02.03>
10. Lehtonen, M. J., Vesa, M., & Harviainen, J. T. (2022). Games-as-a-Disservice: Emergent value co-destruction in platform business models. *Journal of Business Research*, 141, 564–574. <https://doi.org/10.1016/j.jbusres.2021.11.055>
11. Limpach, O. (2020). *The Publishing Challenge for Independent Video Game Developers: A Practical Guide* (1st ed.). CRC Press. <https://doi.org/10.1201/9780367815639>
12. Medvedev, A.I. (2018). Pravovye otnosheniya v prostranstve virtual'nyh igrovyyh mirov: Problemy teorii i praktiki [Legal relations in the space of virtual game worlds: Problems of theory and practice]. *Vestnik Sibirskogo yuridicheskogo instituta Rossii [Vestnik of the Siberian Law Institute of the Ministry of Internal Affairs of Russia]*, (2 (31)), 139–150.
13. Mezei, P., & Harkai, I. (2022). End-user flexibilities in digital copyright law — an empirical analysis of end-user license agreements. *Interactive Entertainment Law Review*, 1–20. <https://doi.org/10.4337/ielr.2022.0003>
14. Newman, J. (2018). The music of microswitches: Preserving videogame sound—a proposal. *The Computer Games Journal*, 7(4), 261–278. <https://doi.org/10.1007/s40869-018-0065-8>
15. Oprysk, L. (2021). Digital consumer contract law without prejudice to copyright: EU digital content directive, reasonable consumer expectations and competition. *GRUR International*, 70(10), 943–956. <https://doi.org/10.1093/grurint/ikab058>
16. Rozhkova, M. A. (2020). Imushchestvennye prava na novye nematerial'nye ob"ekty v sisteme absol'yutnykh prav [Property rights to new intangible objects in the system of absolute rights]. In M. A. Rozhkova (Ed.), *Pravo cifrovoy ekonomiki—2020: Ezhegodnik-antologiya [Law of the Digital Economy—2020: A Yearbook-Antology]* (pp. 5–78). Statut.
17. Saveliev, A. I. (2014). Pravovaya priroda virtual'nyh ob"ektov, priobretaemykh za real'nye den'gi v mnogoprol'zovatel'skikh igrah [Legal nature of virtual objects purchased for real money in multiplayer online games]. *Vestnik grazhdanskogo prava [Civil Law Review]*, 14(1), 127–150.
18. Wiśniewska, K., & Pałka, P. (2024). The impact of the Digital Content Directive on online platforms' Terms of Service. *Yearbook of European Law*, 42, 388–406. <https://doi.org/10.1093/yel/yead004>

Сведения об авторе:

Граф Д. В. — магистрант международно-правового факультета МГИМО МИД России, Москва, Россия.

den29graf2002@gmail.com

ORCID: <https://orcid.org/0009-0001-8360-2140>

Information about the author:

Denis V. Graf — Master Student (LL.M.), International Law Faculty, MGIMO-University, Moscow, Russia.

den29graf2002@gmail.com

ORCID: <https://orcid.org/0009-0001-8360-2140>

СТАТЬИ

БОЛЬШИЕ ДАННЫЕ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ПРАВОВАЯ ПРИРОДА И ВОПРОСЫ РЕГУЛИРОВАНИЯ

С. Н. Тагаева¹, Э. М. Гатиятуллина^{1,2,*}

¹Университет управления «ТИСБИ»
420012, Россия, Казань, ул. Муштары, 11–13

²Научно-исследовательский институт «ВОСХОД»
119607, Россия, Москва, ул. Удальцова, 85

Аннотация

В условиях активного развития цифровых технологий правовое регулирование больших данных (Big Data) и проблемы признания их в качестве объекта гражданского оборота приобретают как теоретическую, так и практическую актуальность. Особую значимость приобретает соотношение больших данных с персональными данными, что порождает необходимость балансирования частных и публичных интересов. Целью данного исследования является проведение комплексного анализа правовой природы больших данных, их соотношения с персональными данными, а также выявление путей совершенствования правовой базы в данной сфере. Исследование направлено на определение возможных подходов к установлению правового режима больших данных, учет особенностей оборота персональных данных как составляющей Big Data и разработку механизмов защиты прав граждан. С опорой на сравнительно-правовой метод авторы уделили особое внимание изучению отечественного и зарубежного законодательства, научных позиций по вопросам правового регулирования больших данных и персональных данных. В результате проведенного исследования установлено, что большие данные имеют неоднородную структуру и включают не только информацию, но и технические устройства, программное обеспечение, обеспечивающие сбор, обработку и анализ данных. Результаты обработки больших данных представляют собой имущественный интерес для субъектов гражданского оборота и могут быть предметом гражданско-правовых договоров. Авторы полагают, что в настоящее время существует конфликт между развитием технологий больших данных и действующим законодательством о персональных данных, что требует создания нового правового механизма для их регулирования. Для успешного внедрения технологий больших данных необходимо обеспечить баланс между защитой персональных данных и возможностями их использования для аналитических целей. В статье подчеркивается необходимость создания нового правового механизма для регулирования больших данных с учетом их специфики и обеспечения баланса между защитой персональных данных и потребностями бизнеса в использовании таких данных для аналитических целей.

Ключевые слова

Big Data, большие данные, персональные данные, правовое регулирование, сбор, обработка, анализ данных, гражданский оборот

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имеет спонсорской поддержки.

Для цитирования

Тагаева, С. Н., Гатиятуллина, Э. М. (2024). Большие данные и персональные данные: правовая природа и вопросы регулирования. *Цифровое право*, 5(2), 40–52. <https://doi.org/10.38044/2686-9136-2024-5-2-40-52>

* Автор, ответственный за переписку

Поступила: 19.04.2024, принята в печать: 22.05.2024, опубликовано: 28.06.2024

ARTICLES

BIG DATA AND PERSONAL DATA: LEGAL CHARACTER AND REGULATORY ISSUES

Sanavbar N. Tagaeva¹, Elmira M. Gatiyatullina^{1,2,*}

¹University of management “TISBI”

11–13, Mushtari str., Kazan, Russia, 420012

²Voskhod Research and Development Institute

85, Udaltsova str., Moscow, Russia, 119607

Abstract

In the context of the rapid development of digital technologies, the legal regulation of Big Data and concomitant recognition as an object of civil circulation acquires both a theoretical and a practical relevance. The particular significance accorded to the relationship between Big Data and personal data involves the need to balance private and public interests. The work sets out to comprehensively analyze the legal character of Big Data and its relationship with personal data to identify approaches for improving the legal framework in this area. Approaches to establishing a legal regime for Big Data take into account specific aspects of the circulation of personal data and the development of mechanisms for protecting citizens' rights. Domestic and foreign legislation is contrasted according to the comparative legal method in the light of jurisprudential positions on the legal regulation of Big Data and personal data. Big Data is shown to have a heterogeneous structure that includes not only information but also technical devices and software that enable the collection, processing, and analysis of data. The results of Big Data processing, which represent a property interest for entities involved in civil transactions, can be the subject of civil law contracts. Conflicts between the development of Big Data technologies and existing personal data legislation necessitate the creation of a new legal mechanism for their regulation. For the successful implementation of Big Data technologies, it is necessary to ensure a balance between the protection of personal data and the opportunities for their use in analytical processes. The creation of a new legal mechanism for regulating Big Data must take into account its specific features to ensure a balance between the protection of personal data and the business needs for using such data for analytical purposes.

Keywords

big data, personal data, legal regulation, collection, processing, data analysis, civil circulation

Conflict of interest The authors declare no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Tagaeva, S. N., & Gatiyatullina, E. M. (2024). Big data and personal data: Legal nature and regulatory issues. *Digital Law Journal*, 5(2), 40–52. <https://doi.org/10.38044/2686-9136-2024-5-2-40-52>

* Corresponding author

Submitted: 19 Apr. 2024, accepted: 22 May 2024, published: 28 June 2024

Активное развитие цифровой среды предоставляет человеку возможность использовать огромные массивы информации из различных источников. Одним из атрибутов цифровой трансформации стали сквозные технологии, среди которых вызывает отдельный интерес такой сложный объект, как *Big Data* — большие данные. Исходя из названия этого явления, предполагается, что речь идет об очень больших объемах информации, которая не может обрабатываться традиционными способами и храниться в обычных базах данных.

Наблюдается усиление внимания к анализу больших данных со стороны участников гражданского оборота с целью прогнозирования спроса и предложения, выбора варианта поведения и сохранения конкурентоспособного преимущества. В частности, путем извлечения необходимых решений из проанализированных массивов данных они корректируют ожидания и строят планы. Анализ больших данных позволяет получить ответ о привлекательности и качестве продукции, запросах потребителей, нарушении прав на результаты интеллектуальной деятельности и др.

Участники гражданского оборота заинтересованы в анализе больших данных и понимают их имущественную ценность. В связи с этим возникает вопрос, в чем же сущность *Big Data* и каков их правовой режим.

Как известно, из-за быстрого темпа технологического прогресса законодателям всё сложнее следить за изменениями в общественных отношениях и реагировать на них вовремя.

В законодательных актах отсутствует стандартное определение категории *Big Data*, или «большие данные», но понятие обработки таких данных раскрывается в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203. Согласно данному документу обработка больших объемов данных представляет собой совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время.

Тем не менее толкование понятия больших данных было дано в приказе Росстата от 31 июля 2024 г. № 332: структурированные и неструктурированные массивы информации, которые характеризуются значительным объемом и высокой скоростью обновления (в том числе в режиме реального времени) данных, что требует специальных инструментов и методов работы с ними (например, машинного обучения, *data* и *text mining* и т.п.)¹.

¹ Приказ Росстата «Об утверждении форм федерального статистического наблюдения для организации федерального статистического наблюдения за деятельностью в сфере образования, науки и инноваций» от 31 июля 2024 г. № 332 (ред. от 30.01.2025).

В Модельном законе о цифровом здравоохранении, который принят 14 апреля 2023 г. в г. Санкт-Петербурге, раскрывается понятие больших данных в сфере медицины. Так, под большими (медицинскими) данными понимаются наборы (медицинских) данных, которые классифицируются в первую очередь по характеристикам объема, разнообразия, скорости и (или) изменчивости и при этом для эффективного хранения, анализа, обработки либо иного управления требуют применения специальной расширенной (масштабируемой) информационной технологии в здравоохранении или информационно-коммуникационной технологии (макротехнологии)².

Таким образом, все имеющиеся разрозненные определения сущности больших данных сходятся в наличии у этих данных нескольких параметров, так называемых 4V: большой объем (*volume*); разнообразие (*variety*); высокая скорость изменения (*velocity*); точность (*veracity*) (VCIOM, 2015, р. 156). Для осуществления обработки больших данных создаются особые распределенные системы хранения данных, которые позволяют использовать внешнее файловое пространство системы хранения для обработки данных на устройствах, входящих в вычислительный кластер. Большие данные активно используются предпринимателями для анализа покупательской способности, прогнозирования и аудиторской деятельности. В настоящее время активное внимание таким данным уделяет и государство.

Следовательно, *Big Data* представляют собой данные, как структурированные, так и неструктурированные, поступающие из множества разнообразных источников. По мнению М. А. Рожковой, большие данные включают все возможные виды данных: *Big Data* — это непрерывно поступающий из разных источников поток огромных объемов разнообразной информации (различных сведений и данных), которые объединяются с уже накопленным колоссальным массивом информации (Rozhkova, 2020, р. 46).

Соглашаясь с тем, что большие данные — это все-таки информация, которая находится в структурированном или неструктурированном виде, необходимо определить в этом потоке данные, являющиеся интересными для субъектов гражданских правоотношений.

Итак, неструктурированные данные, являясь условным понятием, включают в себя необработанные массивы информации общедоступного характера, не отвечающие требованиям конкретности и определенности, которые не могут быть обработаны стандартными базами данных или в системе управления базами данных. Для гражданского оборота интерес представляют структурированные данные, которые обработаны, конкретны, обособлены и представляют имущественный интерес.

Соответственно, составляющие виды информации, формирующие большие данные, могут иметь коммерческую ценность, а могут не обладать таким признаком. В свою очередь, создаваться большие данные могут субъектами гражданского права как в рамках трудовой деятельности (например, базы данных о сотрудниках), так и в личных целях (например, информация из аккаунтов в социальных сетях) или техническими устройствами (например, данные геолокации, данные счетчиков, сенсоров). Как указывали М. А. Рожкова и В. Н. Глонина, технические источники (интернет вещей, промышленный интернет, искусственный интеллект и машинное обучение) создают 90% информации, составляющей большие данные, а социальные источники — лишь 10% (Rozhkova & Glonina, 2020, р. 276).

² Модельный закон о цифровом здравоохранении — участников СНГ, принят 14 апреля 2023 г. в г. Санкт-Петербурге Постановлением 55-2 на 55-м пленарном заседании Межпарламентской ассамблеи государств — участников СНГ). https://iacis.ru/mod_file/p_file/1126

Разнообразие составляющей *Big Data* информации не позволяет говорить о едином правовом режиме данного цифрового актива. На это обстоятельство указывалось в специальной литературе. Так, М. А. Рожкова считает невыполнимой задачей разработку специального правового режима *Big Data*, указывая на наличие градации в представленных в его составе данных (Rozhkova, 2020, p. 47). В силу неоднородности сущности больших данных не сформировалось однозначной позиции и о их правовом режиме.

Тем не менее в науке предложены следующие варианты определения правовой природы и правового режима регулирования больших данных.

1. Одни ученые предлагают рассматривать правовую природу больших данных через призму результатов интеллектуальной деятельности. Так, А. П. Сергеев и Т. А. Терещенко, сравнивая имеющиеся в гражданском законодательстве результаты интеллектуальной деятельности и приравненные к ним объекты, приходят к выводу, что большие данные не являются традиционным объектом интеллектуальной собственности (Sergeev & Tereshchenko, 2018, p. 121). По мнению И. З. Аюшеевой, сбалансированной является позиция, согласно которой большие данные будут признаны в качестве самостоятельно вида сложных объектов интеллектуальных прав (Ayusheyeva, 2023, p. 130). Безусловно, среди большого массива информации могут находиться и объекты, которые являются результатами творческой деятельности, но распространять на весь объем такой информации режим результатов интеллектуальной деятельности неправильно, поскольку природа данных, составляющих *Big Data*, неоднородна. Вместе с тем сбор, анализ и обработка *Big Data* могут осуществляться с помощью средств и методов, которые являются результатами интеллектуальной деятельности.
2. Другие специалисты, отмечая неоднородность структуры больших данных, предлагают рассматривать их как комплекс. Так, Л. Ю. Василевская считает, что *Big Data* являются единым неделимым объектом, идеальным по своей природе, существующим в цифровой форме, в структуре которого выделяются такие элементы, как технологии искусственного интеллекта, программы для ЭВМ (объекты авторского права), программное обеспечение и алгоритмы (ноу-хау), технические решения (изобретения как объекты патентного права), цифровая структурированная информация и др. (Vasilevskaya, 2024, p. 13). При этом она оставляет перечень структурных элементов открытым. А. М. Лаптева, относя большие данные к цифровым активам, склоняется к применению к данному явлению также конструкции имущественного комплекса, который может состоять из 1) информации из «сырых данных» (необработанных данных) и результатов обработки (которые могут быть в том числе в овеществленной форме); 2) имущественных прав (например, исключительных прав на результаты интеллектуальной деятельности, программы для электронных вычислительных машин (программы для ЭВМ), базы данных) (Lapteva, 2019, p. 100–101). Безусловно, такая позиция близка к правовой природе *Big Data*.
3. Третья позиция сводится к пониманию больших данных в качестве информационной услуги по сбору, обработке, аналитике и визуализации больших массивов данных с целью получения необходимой информации и знаний. Множество компаний в сфере информационных технологий и консалтинга предлагают услуги по сбору, анализу и обработке данных, их очистке и структурированию, применению алгоритмов машинного обучения и анализа, интерпретации результатов и предоставлению рекомендаций³. В данном случае не сами *Big Data* являются предметом договора, а результат их обработки, т.е. очищенные, структури-

³ См., например, услуги по обработке данных (<https://www.webformat.ru/services/bigdata/>).

рованные данные, полученные при помощи интеллектуальных способностей специалистов, воздействующих на большие массивы информационных потоков, интересны для участников гражданского оборота.

Анализ представленных позиций показывает, что большие данные нельзя рассматривать как единый объект правового регулирования. Это сложное явление, включающее различные виды информации, каждый из которых может иметь свой правовой режим.

Текущая дискуссия о правовой природе больших данных не привела к формированию единой правовой позиции. Это связано с несколькими факторами: комплексной структурой больших данных, широкой интерпретацией их сущности, которая включает не только информационную составляющую, но и техническую инфраструктуру — оборудование и программные решения, необходимые для обработки и анализа масштабных информационных массивов.

При анализе правового регулирования больших данных и персональных данных необходимо четко разграничивать эти категории. Если правовой режим персональных данных определен законодательством и имеет ясную структуру регулирования, то большие данные представляют собой более широкое явление, включающее различные виды информации с разным правовым режимом. При этом персональные данные могут быть частью больших данных, но не наоборот. Такое разграничение важно для правильного применения соответствующих правовых норм и механизмов защиты прав субъектов.

При рассмотрении проблемы больших данных следует учитывать два момента: во-первых, большие данные — это информация, которая получена для анализа и обработки или получена в результате анализа и обработки с помощью технических устройств и программного обеспечения; во-вторых, это технологии обработки больших данных. Именно «невозможность существования *Big Data* без своего материального носителя — компьютерного устройства с соответствующим программным обеспечением (совокупностью определенных программ) и искусственным интеллектом (новым инновационным продуктом интеллектуальной деятельности)» (Vasilevskaya, 2024, p. 13) позволила обозначать термином «большие данные» не только объект — информацию, но и методы и способы воздействия на объект. На данный момент сложно говорить о правовом режиме больших данных, поскольку большие массивы разнородной информации не являются обособленными и однородными; за исключением отдельных составляющих, программные инструменты, используемые для обработки и анализа информации, являются результатами интеллектуальной деятельности. На данный момент нет необходимости определять правовой инструментарий, который позволит достичь правовых целей регулирования и социально значимого результата всего комплекса больших данных, соответственно, неактуален вопрос о защите прав на такой многоаспектный объект. В свою очередь, представляет интерес установление правового режима с учетом его специфики для каждого отдельного элемента, составляющего большие данные.

Другой момент, на который стоит обратить внимание, — то, что результат сбора, анализа и обработки больших данных представляет имущественный интерес для субъектов гражданского оборота и может быть предметом гражданско-правовых договоров, в связи с чем в науке аргументируется необходимость конкретно-определенной регламентации договорных условий и ограничений деятельности по сбору, обработке, использованию данных (Antipova, 2021, p. 157).

Естественно, использование технологии больших данных не должно нарушать имеющиеся режимы по защите прав субъектов правоотношений, и в фокусе правового регулирования должно быть обеспечение баланса интересов участников правоотношений.

Актуальной проблемой является достаточная и необходимая модель регулирования отношений, связанных с большими данными, которые могут содержать в себе и персональные данные граждан. В силу того, что одной из составляющих больших данных являются персональные данные физических лиц, для которых законодательство установило режим ограниченного доступа, состав *Big Data* разнороден, соответственно, включает в себя объекты с различным режимом правового регулирования. Но наиболее урегулированной составляющей больших данных являются именно персональные данные, к обработке которых законодательство предъявляет особые требования.

В современной российской правовой системе «персональные данные» представляют собой сложную и многогранную правовую категорию, имеющую принципиальное значение для защиты прав и свобод граждан. Правовая природа персональных данных определяется комплексом нормативно-правовых актов, среди которых ключевую роль играет Федеральный закон «О персональных данных»⁴.

Юридическая сущность персональных данных заключается в их особом статусе как информации, напрямую связанной с конкретным физическим лицом и требующей специального правового режима обработки и защиты. Принципиальными характеристиками персональных данных являются:

- 1) индивидуализация субъекта, возможность прямой или косвенной идентификации личности;
- 2) строго целевой характер сбора и обработки информации;
- 3) необходимость получения согласия субъекта на обработку персональных данных.

Правовой режим персональных данных предусматривает жесткие требования к их сбору, хранению, передаче и уничтожению. Операторы персональных данных несут полную юридическую ответственность за нарушение установленного порядка, включая административную и уголовную ответственность.

Важным аспектом правовой природы персональных данных является их деление на общедоступные и конфиденциальные, что определяет различные режимы правовой защиты. Особо чувствительные категории персональных данных, такие как биометрические или данные о состоянии здоровья, имеют максимально строгий режим правовой охраны. Так, согласно п. 3 ст. 3 Федерального закона «О персональных данных» под обработкой персональных данных понимается любое действие или совокупность таких действий, которые совершаются как с использованием средств автоматизации, так и без их использования, включая сбор, запись, систематизацию, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Исходя из этого определения можно сделать вывод о том, что любое действие с персональными данными будет являться их обработкой.

Каким образом законодательство Российской Федерации регулирует оборот персональных данных в контексте использования технологий больших данных, которые позволяют обрабатывать и анализировать информацию не только о производственных процессах, но и о физических лицах (субъектах персональных данных)?

При анализе условий обработки персональных данных следует уделить особое внимание принципам законности, ограничения цели обработки и минимизации обрабатываемых данных в свете использования технологий больших данных. Данные принципы выбраны исходя из следующих оснований: при обработке особых категорий персональных данных возникает вопрос

⁴ Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ. СЗ РФ, 31.07.2006. № 31 (ч. 1). Ст. 3451.

законности обработки таких данных, соответствия целей сбора таких данных целям обработки, минимизации персональных данных, в том числе возможности их обезличивания при осуществлении обработки. Кроме того, предлагается рассмотреть возможность принятия решений на основании исключительно автоматизированной обработки персональных данных с использованием технологии больших данных.

Согласно ст. 5 Федерального закона «О персональных данных» содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, а также обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

На аналогичных положениях базируется правовая база о персональных данных некоторых зарубежных стран и их объединений. Например, в ст. 5 Регламента № 2016/679 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» закреплено, что персональные данные должны собираться для конкретных, отчетливых и законных целей и не обрабатываться в последующем несовместимым с этими целями образом⁵.

Для обеспечения принципа прозрачности обработки персональных данных в контексте больших данных оператор или контроллер должен обеспечить ясное и понятное предоставление информации субъектам о целях обработки их данных. Это предполагает разработку и документирование политики обработки персональных данных и согласий с учетом требований законодательства. Осуществление контроля над данными способствует взаимному доверию между оператором и субъектом, а также позволяет субъекту сохранять осведомленность и управление своими данными, включая обработку больших объемов информации.

Тем не менее технологии машинного обучения зачастую выходят за пределы одной поставленной цели обработки, в связи с чем оператор каждый раз при обнаружении в рамках своих систем больших данных новых целей и способов обработки должен уведомлять субъектов персональных данных об изменениях.

Если процесс обработки персональных данных не будет проводиться со строгим соблюдением установленных целей и методов, это может привести к нарушению требований законности обработки и привлечению к ответственности согласно отечественному и европейскому (в случае, если в массив больших данных попали персональные данные граждан Европы) законодательству. При изменении целей обработки необходимо учитывать также категорию обрабатываемых данных, поскольку законом запрещено использование персональных данных для других целей, не предусмотренных на начальном этапе и не совместимых с изначальной целью. Действительно, существуют определенные исключения и цели обработки персональных данных, которые могут быть рассмотрены как совместимые с первоначальной целью сбора данных: публичные интересы, научные или исторические исследования и статистические цели.

Впрочем, операторы должны строго следовать законодательству о персональных данных и соблюдать принципы обработки данных, такие как прозрачность, аккуратность и надежность. Лазейки в регулировании обработки больших данных не должны использоваться для обхода закона или нарушения прав граждан. Если оператор планирует использовать персональные данные для целей, не указанных в изначальном согласии субъекта данных, необходимо провести анализ совместимости новых целей с целями первоначальной обработки. В случае

⁵ Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to The Processing of Personal Data and On the Free Movement of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ (L 119).

сомнений или разногласий рекомендуется получить согласие субъекта данных на новую цель обработки. В целом необходимо тщательно и ответственно подходить к обработке персональных данных, соблюдая законы и права граждан на защиту их личной информации.

Такое исключение сделано, например, для обработки персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, которое допускается в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных федеральными законами от 24 апреля 2020 г. № 123-ФЗ⁶ и от 31 июля 2020 г. № 58-ФЗ⁷, в порядке и на условиях, которые установлены указанными федеральными законами. Однако речь идет об обезличенных данных, таким образом, обработка персональных данных в рамках получения статистических данных без обезличивания запрещена.

Следует отметить, что использование больших данных для юридически значимых решений требует особой осторожности. Важно понимать, что обработка данных с целью статистического анализа и использование их для принятия решений, например в сфере таргетированной рекламы, имеют различные правовые последствия. Поэтому необходимо учитывать этот нюанс при использовании больших данных для конкретных целей. Например, в Федеральном законе «О персональных данных» прямо запрещено использование персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации без предварительного согласия на такую обработку.

Одним из важных принципов целевого ограничения является обязанность оператора не допускать объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Более того, согласно ст. 25 Регламента № 2016/679 и ст. 18.1 Федерального закона «О персональных данных», оператор должен применять соответствующие технические и организационные меры для обеспечения этого. В рамках больших данных, представляющих собой не структурированную в привычном понимании базу данных, такое практически невозможно и как минимум экономически нецелесообразно.

С учетом принципа минимизации данных оператор должен обрабатывать только те данные, которые необходимы и достаточны для достижения обозначенных целей. Исходя из прямого указания Федерального закона «О персональных данных», обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. Сбор персональных данных должен быть ограничен конкретным объемом сведений, который необходим для достижения заявленных целей обработки. С учетом данного принципа недопустимо собирать сведения в большем объеме в надежде, что эти данные когда-нибудь пригодятся. Возникает правовая коллизия между принципом больших данных и принципом минимизации персональных данных. Данное несоответствие неоднократно отмечали исследователи, например С. В. Соловкин (Solovkin, 2023, p. 97) и О. Л. Алферов (Alferov, 2023, p. 169), поскольку сама основа больших данных заключается в сборе как можно большего количества персональных данных за единицу времени.

⁶ Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» от 24 апреля 2020 г. № 123-ФЗ. СЗ РФ, 27.04.2020, № 17, ст. 2701.

⁷ Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31 июля 2020 г. № 258-ФЗ. СЗ РФ, 03.08.2020, № 31 (часть I), ст. 5017.

Кроме того, возникают вопросы относительно принципа минимизации хранения информации в связи с постоянным развитием технологий обработки данных. Возможность альтернативного анализа уже собранных данных подразумевает необходимость их долгосрочного хранения оператором. Механизм исключения обработки данных для статистических целей ограничивает применение данного принципа в контексте больших данных. Рекомендуется изменение правового регулирования использования принципа минимизации данных в отношении больших данных, включая регулирование отдельных аспектов обработки персональных данных, входящих в состав больших данных.

Основной принцип, отраженный в ст. 6 Федерального закона «О персональных данных», — это наличие правового основания для обработки персональных данных: либо личное согласие, либо законное основание для обработки без наличия согласия на обработку. В случае с технологиями больших данных получение согласия на обработку у каждого субъекта персональных данных затруднительно. В соответствии со ст. 9 Федерального закона «О персональных данных» согласие должно содержать большой перечень реквизитов и должно быть дано в форме отдельного документа, а не в качестве, например, приложения к договору, что усложняет обработку информации с помощью больших данных.

Эксплуатация больших данных может привести к тому, что результаты анализа данных будут содержать категории персональной информации, которые ранее не рассматривались как таковые. Например, анализ списка покупок может раскрывать информацию о здоровье человека, что подпадает под специальную категорию персональных данных. Технологии больших данных обладают свойством сглаживать различия между разными категориями персональных данных. С учетом этой особенности необходимо пересмотреть правовое регулирование для сбалансированного учета интересов предпринимателей, обрабатывающих большие данные, и общественных интересов защиты персональных данных различных категорий.

В связи с тем, что в системах обработки больших данных накапливается значительный объем информации о гражданине, важно определить правовой режим такой информации и механизмы защиты прав субъектов персональных данных. Персональные данные, являясь нематериальным благом, не могут быть объектом права собственности согласно доктрине российского гражданского права. Вместо этого следует говорить о комплексе прав субъекта персональных данных на защиту и контроль за их обработкой, а также об обязанностях операторов по обеспечению их безопасности. При этом результаты обработки и анализа персональных данных могут представлять коммерческую ценность для операторов таких систем, что создает необходимость поиска баланса между правами субъектов персональных данных и интересами операторов.

В данной ситуации практически неизбежен конфликт частноправовых интересов граждан и правовых интересов операторов и заказчиков такой обработки. Наиболее эффективным средством минимизации подобных рисков, как справедливо отмечается в научной литературе, является право во всех проявлениях. В этой связи видится необходимым создание правовых и технических условий для обеспечения защиты персональных данных граждан, передаваемых и обрабатываемых в массивах *Big Data*.

Еще одна проблема, на которую хотелось бы обратить внимание, — это автоматическое принятие решений исключительно с помощью результата обработки больших данных: довольно сложно соблюсти требования законодательства о персональных данных в рамках использования машинного обучения с целью последующего автоматизированного принятия решений. Коллизия заключается в необходимости получить согласие на принятие решений на основе анализа персональных данных наряду с необходимостью разъяснить субъектам процедуру

принятия таких решений, что создает предпосылки для нарушения операторами законодательства. Коммерческая тайна процесса принятия решений, основанного на алгоритмах машинного обучения, затрудняет его объяснение, что может привести к нарушению требований о прозрачности и информировании. Кроме того, отсутствие понимания принципов работы машинного обучения среди сотрудников усугубляет ситуацию и усложняет выполнение законных требований. В результате возникают серьезные риски для развития применения больших данных в различных сферах экономики. В текущей ситуации указанная норма неэффективна, что приводит к тому, что используемые современные технологии обработки больших данных сталкиваются с проблемой необходимости соблюдения законодательства о персональных данных. На сегодняшний день, с одной стороны, нарушение правил обработки персональных данных может привести к серьезным штрафам для организаций. С другой стороны, аналитики и исследователи нуждаются в доступе к большому объему данных для проведения анализа и выявления закономерностей.

Особого внимания заслуживает эволюция правового регулирования обезличенных данных в российском законодательстве. С 1 сентября 2025 г. вступает в силу Федеральный закон «О внесении изменений в Федеральный закон “О персональных данных” и Федеральный закон “О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”»⁸, основной целью которого являются уменьшение объема оборота обрабатываемых персональных данных и повышение их защищенности при осуществлении обработки данных с использованием новых технологий, а также регулирования оборота больших объемов данных.

Указанный Закон вносит значительные корректировки в понимание и регулирование обезличенных данных, что напрямую влияет на использование технологий больших данных. Ключевым изменением становится новый подход к определению обезличенных данных и требованиям к процессу обезличивания. Законодатель уточняет, что обезличенные персональные данные — это информация, которая получена в результате обезличивания персональных данных и не позволяет без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Это определение существенно влияет на возможности использования больших данных в аналитических целях.

Важным нововведением является детальная регламентация обезличивания данных. Это создает новые правовые рамки для операторов больших данных, которым необходимо будет адаптировать свои процессы под новые требования. Текущая методика обезличивания персональных данных, утвержденная приказом Роскомнадзора, требует переосмысления в контексте современных технологий обработки данных⁹. Существующие методы (метод введения идентификаторов, метод изменения состава или семантики, метод декомпозиции, метод перемешивания) не всегда эффективны при работе с большими данными, особенно когда речь идет о машинном

⁸ Федеральный закон «О внесении изменений в Федеральный закон “О персональных данных” и Федеральный закон “О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”» от 8 августа 2024 г. № 233-ФЗ. СЗ РФ, 12.08.2024, № 33 (Часть I), ст. 4929.

⁹ Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13 декабря 2013 г.).

обучении и использовании искусственного интеллекта. В связи с этим особое значение приобретают разрабатываемые подзаконные акты, которые должны детализировать требования Закона. В частности, ожидается принятие нормативных актов, определяющих технические требования к процессу обезличивания персональных данных, а также методы контроля эффективности обезличивания.

Для нахождения баланса между обеспечением защищенности персональных данных и потребностями аналитиков необходимо разработать и применять гибкие и сбалансированные правила и механизмы регулирования. Законодателям следует учитывать не только потребности компаний и организаций в обработке данных, но и защиту прав и интересов граждан. Правоприменителям же необходимо контролировать соблюдение законодательства и в случае нарушений принимать соответствующие меры.

В контексте развития правового регулирования больших данных необходимо обратить внимание на несколько ключевых аспектов современного нормотворчества и правоприменения. Проект федерального закона «О промышленных данных» представляет особый интерес, поскольку вводит новую категорию данных и механизмы их регулирования. Законопроект направлен на установление правового режима промышленных данных, определение прав и обязанностей субъектов, участвующих в их обороте. Это создает дополнительный уровень сложности в разграничении различных категорий данных и их правовых режимов.

Отдельного внимания заслуживает вопрос о достаточности положений ГК РФ в части регулирования баз данных применительно к массивам больших данных. Действующие нормы гл. 71 ГК РФ, регулирующие права на базы данных, не в полной мере учитывают специфику больших данных. В частности, критерий творческого характера подбора и организации материалов, необходимый для предоставления авторско-правовой охраны, плохо применим к автоматически генерируемым массивам данных и использованию технологий искусственного интеллекта. Помимо этого, существующие нормы не учитывают динамический характер больших данных и особенности их автоматизированной обработки.

Таким образом, для эффективной работы в области обработки больших данных необходимо учитывать и соблюдать требования законодательства о персональных данных, обеспечивая защиту данных граждан и одновременно возможность использования данных для целей аналитики и исследований.

Список литературы / References

1. Alferov, O. L. (2023). Bol'shiye dannye v yuridicheskoy deyatel'nosti [Big data in legal practice]. *Sotsial'nyye i gumanitarnyye nauki. Otechestvennaya i zarubezhnaya literatura. Ser. 4, Gosudarstvo i pravo* [Social Sciences and Humanities. Domestic and Foreign Literature. Series 4: State and Law], (3), 165–176. <https://10.31249/iajpravo/2023.03.14>
2. Antipova, K. G. (2021). Sposoby opredeleniya bol'shikh dannykh: Rossiyskiy i zarubezhnyy opyt [Methods of big data definition: russian and foreign experience]. *Yuridicheskiye issledovaniya* [Legal Studies], (9), 143–157. <https://10.25136/2409-7136.2021.9.3659>
3. Ayusheva, I. Z. (2023). Bol'shiye dannyye: problemy opredeleniya grazhdansko-pravovogo rezhima [Big data: problems of defining the civil law regime]. *Lex Russica*, 77(10), 125–134. <https://doi.org/10.17803/1729-5920.2023.203.10.125-134>
4. Vasilevskaya, L. Yu. (2024). Big data v mekhanizme formirovaniya osnovnykh napravleniy natsional'nogo proyekta “Ekonomika dannykh”: vzglyad tsivilista na problemu [Big Data in the mechanism of the formation of the project “Economy of data”: a civilist's view on the problem]

- of main directions of the “Data Economy” national project: A civilist’s view of the problem]. *Lex Russica*, 77(1), 9–21. <https://doi.org/10.17803/1729-5920.2024.206.1.009-021>
5. VCIOM. (2015). V mezhdunarodnaya sotsiologicheskoy Grushinskoy konferentsii “Bol’shaya Sotsiologiya: Rasshireniye prostranstva dannykh” Izbrannyye tezisy k sektsii Sotsiologiya i Big Data [V international sociological conference “Big Sociology: Expansion of Data Space” Selected abstracts for the Sociology and Big Data section]. *Monitoring obshchestvennogo mneniya: ekonomicheskiye i sotsial’nyye peremeny* [Monitoring of Public Opinion: Economic and Social Changes], (3), 138–154. <https://www.monitoringjournal.ru/index.php/monitoring/article/view/1217>
 6. Lapteva, A. M. (2019). Pravovoy rezhim tsifrovyykh aktivov (na primere Big Data) [Legal regime of the digital assets (on example of Big Data)]. *Zhurnal rossiyskogo prava* [Journal of Russian Law], (4), 93–104.
 7. Rozhkova, M. A. (2020). Imushchestvennye prava na novye nematerial’nye ob’ekty v sisteme absolyutnykh prav [Property rights to new intangible objects in the system of absolute rights]. In M. A. Rozhkova (Ed.), *Pravo cifrovoy ekonomiki—2020: Ezhegodnik-antologiya* [Law of the Digital Economy—2020: A Yearbook-Antology] (pp. 5–78). Statut.
 8. Rozhkova, M. A., & Glonina, V. N. (2020). Personal’nyye i nepersonal’nyye dannyye v sostave bol’shikh dannykh [Personal and non-personal data as part of big data]. In M. A. Rozhkova (Ed.), *Pravo tsifrovoy ekonomiki — 2020* (16) (pp. 271–298). Statut.
 9. Sergeev, A. P., & Tereshchenko, T. A. (2018). Bol’shiye dannye: v poiskakh mesta v sisteme grazhdanskogo prava [Big data: In search of a place in the civil law system]. *Zakon*, (11), 106–123.
 10. Solovkin, S. V. (2023). Avtomatizirovannyi sbor dannykh o cheloveke: neyavnyye printsipy pravovogo regulirovaniya [Automated collection of data on a person: Implicit principles of legal regulation]. *Courier of Kurfan Moscow State Law University (MSAL)*, (2), 90–100. <https://doi.org/10.17803/2311-5998.2023.102.2.090-100>

Сведения об авторах:

Тагаева С. Н. — доктор юридических наук, профессор, профессор кафедры гражданского и предпринимательского права, Университет управления «ТИСБИ», Казань, Россия.

s.tagaeva@mail.ru

ORCID: <https://orcid.org/0000-0002-8831-9344>

Гатиятуллина Э. М. — аспирант кафедры гражданского и предпринимательского права, Университет управления «ТИСБИ», заместитель руководителя Правового департамента, Научно-исследовательский институт «ВОСХОД», Москва, Россия.

askoelm@mail.ru

ORCID: <https://orcid.org/0009-0004-4545-7132>

Information about the authors:

Sanavbar N. Tagaeva — Dr. Sci. in Law, Professor, Professor of the Department of Civil and Business Law, University of management “TISBI”, Kazan, Russia.

s.tagaeva@mail.ru

ORCID: <https://orcid.org/0000-0002-8831-9344>

Elmira M. Gatiyatullina — Postgraduate student, Department of Civil and Business Law, University of management “TISBI”, Deputy Head of the Legal Department, Voskhod Research and Development Institute, Moscow, Russia.

askoelm@mail.ru

ORCID: <https://orcid.org/0009-0004-4545-7132>

ОБЗОРНЫЕ СТАТЬИ

ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ЦИФРОВОГО ОБЪЕКТА И ЦИФРОВОГО АКТИВА

А. Г. Шипикова^{1,2}

¹Московский государственный институт международных отношений
(университет) МИД России
119454, Россия, Москва, пр. Вернадского, 76

²Московский городской суд
107076, Россия, Москва, ул. Богородский Вал, 8

Аннотация

Развитие цифровых технологий привело к появлению новых объектов права и правоотношений, осмысление которых необходимо для обеспечения реализации прав и основных свобод человека, в том числе права собственности и права на уважение человеческого достоинства. Среди основных объектов, возникших в результате развития цифровых технологий, цифровые объекты и активы. Цель настоящей статьи — предпринять попытку сформулировать понятие «цифровой объект», провести сравнительное исследование подходов к определению понятия «цифровой актив», выделить ключевые признаки понятия «цифровой актив», предложить подходы к определению соотношения понятий «цифровой объект» и «цифровой актив», что будет способствовать развитию правового регулирования в условиях цифровизации общества. В ходе исследования проанализированы подходы к определению понятий «цифровой объект» и «цифровой актив», содержащиеся в доктринальных источниках как в Российской Федерации, так и за рубежом (США, Великобритании, Германии). Проведен анализ указанных категорий, содержащихся в нормативных источниках, в том числе на уровне международных организаций и межгосударственных интеграционных объединений. При исследовании использовались догматический и формально-логический методы, аксиологический подход и метод сравнения. По итогам проведенного анализа предложены определения понятий «цифровой объект», «цифровой актив», подходы к их соотношению. Выделены существенные характеристики такой категории, как «цифровой актив», на основе материалов, разработанных на уровне Международного института унификации частного права (УНИДРУА), СНГ, Европейского института права, проанализированы общие черты и различия понятий «цифровой объект» и «цифровой актив». Сформулирован вывод о том, что цифровой объект можно рассматривать как общее, родовое понятие, включающее в себя в том числе цифровые активы и другие объекты, например аккаунты в социальных сетях, аккаунты электронной почты, при этом, существенным, конституирующим признаком цифрового актива является понятие контроля в отношении цифрового актива.

Ключевые слова

цифровой объект, цифровой актив, цифровизация, правовое регулирование, права человека, право собственности, частное право

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имеет спонсорской поддержки.

Для цитирования

Шипикова, А. Г. (2024). Подходы к определению цифрового объекта и цифрового актива. *Цифровое право*, 5(2), 53–68. <https://doi.org/10.38044/2686-9136-2024-5-2-1>

Поступила: 02.04.2024, принята в печать: 03.05.2024, опубликовано: 28.06.2024

REVIEW ARTICLES

CONCEPTUAL APPROACHES TO DEFINING DIGITAL OBJECTS AND DIGITAL ASSETS

Anna G. Shipikova^{1,2}

¹Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

²Moscow City Court
8, Bogorodsky Val str., Moscow, Russia, 107076

Abstract

The development of digital technologies has led to the emergence of new objects of law and legal relations, the understanding of which is necessary to ensure the implementation of human rights and fundamental freedoms, including the right to property and the right to respect for human dignity. Among the main objects that have arisen as a result of the development of digital technologies are digital objects and assets. The purpose of this article is to attempt to formulate the concept of a “digital object”, conduct a comparative study of approaches to defining the concept of a “digital asset”, highlight the key features of the concept of a “digital asset”, propose approaches to determining the relationship between the concepts of a “digital object” and a “digital asset”, which will contribute to the development of legal regulation in the context of the digitalization of society. The approaches to defining the concepts of a “digital object” and a “digital asset” contained in doctrinal sources both in the Russian Federation and abroad (USA, Great Britain, Germany) are analyzed. An analysis of these categories contained in regulatory sources, including at the level of international organizations and interstate integration associations, is carried out. The study used dogmatic and formal-logical methods, an axiological approach and a comparison method. Based on the results of the analysis, definitions of the concepts of “digital object”, “digital asset”, and approaches to their relationship are proposed. The essential characteristics of such a category as “digital asset” are identified based on the materials developed at the level of the International Institute for the Unification of Private Law (UNIDROIT), the CIS, and the European Institute of Law, and the common features and differences between the concepts of “digital object” and “digital asset” are analyzed. A conclusion is formulated that a digital object can be considered as a general, generic concept that includes digital assets and other objects, such as social media accounts, email accounts, while an essential, constitutive feature of a digital asset is the concept of control over a digital asset.

Keywords

digital object, digital asset, digitalization, legal regulation, human rights, property rights, private law

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Shipikova, A. G. (2024). Conceptual approaches to defining digital objects and digital assets. *Digital Law Journal*, 5(2), 53–68. <https://doi.org/10.38044/2686-9136-2024-5-2-1>

Submitted: 2 Apr. 2024, accepted: 3 May 2024, published: 28 June 2024

Введение

Современное общество характеризуется возрастающим использованием цифровых технологий, что позволяет говорить о цифровизации общества. Цифровизация — процесс организации осуществления в цифровой среде функций и деятельности, ранее выполнявшихся без использования цифровых продуктов, предполагающий внедрение в отдельные аспекты соответствующей деятельности информационно-телекоммуникационных технологий, а применительно к экономической деятельности и государственному управлению предусматривающий, в частности, внедрение и (или) применение цифровых технологий, обеспечивающих повышение эффективности указанных деятельности и управления¹.

В зарубежных источниках указывается, что цифровизация является одной из наиболее значительных трансформаций современного общества и охватывает многие элементы бизнеса и повседневной жизни (Kraus et al., 2022, p. 1). Цифровизация означает как переход от «аналогового» к «цифровому» (например, от наличных денег к электронным платежам), так и содействие новым формам создания стоимости (Hagberg et al., 2016, p. 696). Цифровизация — это способ реструктуризации многих сфер социальной жизни вокруг цифровых коммуникационных и медиаинфраструктур (Brennen & Kreiss, 2016, p. 1). Проще говоря, цифровизацию можно определить как использование цифровых технологий (Srai & Lorentz, 2019, p. 79).

Право собственности является одной из составляющих правового статуса личности. Международно-правовое признание права собственности как одного из прав человека на современном этапе берет начало во Всеобщей декларации прав человека 1948 г., в соответствии со ст. 17 которой каждый человек имеет право владеть имуществом как единолично, так и совместно с другими. Никто не должен быть произвольно лишен своего имущества².

В дальнейшем право собственности в качестве права человека получило нормативное закрепление, в частности, в Конвенции о защите прав человека и основных свобод 1950 г.,

¹ Модельный закон о цифровой трансформации отраслей промышленности государств — участников СНГ, принят 14 апреля 2023 г. в г. Санкт-Петербурге Постановлением 55-9 на 55-м пленарном заседании Межпарламентской ассамблеи государств — участников СНГ). https://iacis.ru/mod_file/p_file/1111

² Всеобщая декларация прав человека: принята Генеральной Ассамблеей ООН 10 декабря 1948 г. // Российская газета. — 1995. — 05 апреля.

в соответствии со ст. 1 Протокола № 1 к которой каждое физическое или юридическое лицо имеет право на уважение своей собственности. Никто не может быть лишен своего имущества иначе как в интересах общества и на условиях, предусмотренных законом и общими принципами международного права³.

Право на уважение частной жизни также является одним из фундаментальных прав человека и также берет начало во Всеобщей декларации прав человека 1948 г. (ст. 12)⁴. В дальнейшем указанное право было нормативно закреплено в таких международно-правовых актах, как Международный пакт о гражданских и политических правах 1966 г. (ст. 17), Конвенция о защите прав человека и основных свобод (ст. 8).

Если говорить о праве собственности в условиях цифровизации и в отношении цифровых объектов, то нельзя не сказать о наличии различных подходов к данному вопросу. Так, как указывает А.А. Иванов в статье «Цифровизация и вещные права. Фрагмент из цикла лекций “Гражданское право и цифровизация”», тот факт, что в российском законодательстве «не признано, что объекты вещных прав — вещи с четкими пространственными границами, создает методологическую основу для подведения под вещно-правовое регулирование чего-то бестелесного и в целом относящегося к совершенно иным сферам правового регулирования» (Ivanov, 2023, p. 44). То есть имеются основания для того, чтобы рассматривать цифровые объекты как особого рода объекты вещного права и в связи с этим применять соответствующее гражданско-правовое регулирование.

С другой стороны, нельзя не учитывать и наличие особой специфики цифровых объектов, что не позволяет относить их к объектам права собственности или иных вещных прав в их классическом понимании. Прежде всего это связано именно с нематериальным характером цифровых объектов и с необходимостью определенных технических средств для реализации прав на указанные объекты.

Кроме того, правовой режим таких цифровых объектов, как, например, аккаунты в социальных сетях, учетные записи электронной почты, права доступа в облачные хранилища и т.п., тесно связан с правом на уважение частной жизни, что подтверждается в том числе законодательством ряда государств и соответствующей судебной практикой. В настоящей работе анализируются понятия цифрового объекта и цифрового актива и их соотношение в том числе с использованием зарубежного нормативного и доктринального материала, а также материалов международных интеграционных объединений.

Обзор литературы, постановка проблемы

В научной литературе часто используются понятия цифрового объекта и цифрового актива. Для целей дальнейшего исследования целесообразно определить указанные категории с точки зрения гражданского права.

Понятие «цифровой объект» применительно к сфере гражданского оборота в западной литературе недостаточно распространено. В многочисленных источниках о цифровых

³ Конвенция о защите прав человека и основных свобод (заключена в г. Риме 4 ноября 1950 г.), вместе с Протоколом [№ 1] (подписан в г. Париже 20 марта 1952 г.) // Собрание законодательства РФ. — 2001. — № 2. — Ст. 163.

⁴ В соответствии со ст. 12 Декларации «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

объектах говорится только в чрезвычайно узком, специальном смысле (Hui, 2012, p. 380; Koles & Nagy, 2021, p. 60; Lyons, 1997, p. 22), как, например, об объектах, выраженных последовательностью байтов или битов (Faulkner & Runde, 2019, p. 1285); указывается на такие свойства цифровых объектов, как возможность их редактирования, интерактивность, возможность получения доступа к таким объектам и их изменения с помощью других цифровых объектов, распределенность цифровых объектов. Таким образом, согласно общепринятой доктрине, цифровые объекты представляют собой не более чем временные «сборки» функций, информационных элементов или компонентов, распределенных по информационным инфраструктурам и Интернету (Kallinikos et al., 2010, p. 5).

При использовании понятия «цифровой объект» в западной литературе, как правило, имеют в виду совокупность различного рода объектов, размещенных в сети Интернет (фото, видео, тексты, различного рода гипертекстовые, мультимедийные и интерактивные материалы и т.п.). Применительно к сфере гражданского оборота в западной литературе гораздо более распространено понятие «цифровой актив», как будет продемонстрировано ниже.

Что касается российской доктрины, то в научных источниках используются понятия как «цифровой объект», так и «цифровой актив», и порой объемы этих понятий в том контексте, в котором их используют авторы, в большей части совпадают (Volos, 2022).

Исключение составляют научные работы, в которых проводится анализ недавно принятых федеральных законов, посвященных правовому регулированию цифровых финансовых активов (Melnikova et al., 2023). Также в докладах регулятора, специально посвященных обороту именно финансовых активов, используется термин «цифровой актив»⁵.

В ряде работ российских ученых выражаются различные подходы к правовой природе и режиму цифровых объектов и цифровых активов. Речь идет о трудах И. З. Аюшеевой (Ayusheeva, 2021), В. Е. Величко, Э. А. Евстигнеева (Velichko & Evstigneev, 2019), М. А. Рожковой⁶, Е. А. Суханова (Sukhanov, 2021). Некоторые аспекты цифровых объектов были освещены в фундаментальной работе К. И. Скловского (Sklovskiy, 2023, p. 273). В статье Д. А. Т. Фэйрфилда также рассматриваются вопросы, связанные с цифровыми объектами, особо акцентируется внимание на понятии контроля применительно к цифровым объектам (Fairfield, 2023, p. 22). Между тем анализ вышеупомянутых исследований показывает, что авторы используют различные подходы к указанным понятиям, рассматривают их с различных точек зрения.

Указанное свидетельствует о непроработанности в целом теории цифровых объектов и об отсутствии консенсуса относительно содержания понятий цифровой объект и цифровой актив, а также их соотношения.

⁵ Центральный банк Российской Федерации. (2022). Развитие рынка цифровых активов в Российской Федерации: доклад для общественных консультаций. https://cbr.ru/Content/Document/File/141991/Consultation_Paper_07112022.pdf; Центральный банк Российской Федерации. (2022). Криптовалюты: тренды, риски, меры: доклад для общественных консультаций. https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf

⁶ Rozhkova, M. A. (2019, January 14). *Ob imushchestvennykh pravakh na nematerial'nyye ob"yekty v sisteme absol'yutnykh prav (chast' tret'ya — prava na svedeniya i dannyye kak raznovidnosti informatsii)* [On property rights to intangible objects in the system of absolute rights (part three — rights to information and data as types of information)]. *Zakon.ru*. https://zakon.ru/blog/2019/1/14/ob_imushchestvennykh_pravakh_na_nematerialnye_obekty_v_sisteme_absolyutnykh_prav_chast_tretya_prava_na

Подходы к определению понятий «цифровой объект» и «цифровой актив»

Понятийный аппарат, в том числе категории цифрового объекта и цифрового актива и их соотношение, проработан в модельных законах, принятых Межпарламентской ассамблеей государств — участников СНГ, в частности в Модельном законе «О цифровых правах»⁷.

В соответствии с абз. 15 ст. 3 указанного Модельного закона «цифровой объект — не имеющий вещественного выражения объект гражданских прав, доказательства существования которого формируются и обладатель которого определяется посредством кодирования информации в информационно-коммуникационной среде с помощью записей в информационной системе по ее правилам». При этом под цифровым активом в данной статье понимается в том числе и виртуальный актив, токен — «цифровой объект, обладающий имущественной ценностью (имущество), право собственности или другое вещное право на который принадлежит субъекту, указанному в информационной системе в качестве его обладателя» (абз. 12 ст. 3 Модельного закона).

В понятийной системе указанного Модельного закона «цифровой объект» и «цифровой актив» соотносятся как общее и частное, как родовое и видовое понятия.

В целом подобный подход оправдан, так как понятие «цифровой объект» очевидно является более широким и родовым по отношению к более узкому понятию цифрового актива, определяемого через видовое отличие — как цифровой объект, обладающий имущественной ценностью и принадлежащий обладателю на праве собственности или другом вещном праве.

Таким образом, основным отличием цифрового актива от цифрового объекта, согласно вышеуказанному Модельному закону, является то, что цифровой актив, во-первых, является объектом, имеющим имущественную ценность, и, во-вторых, принадлежит обладателю на праве собственности или другом вещном праве. Между тем понятие цифрового объекта включает и многие другие объекты, которые могут имущественной ценностью не обладать и в отношении которых можно осуществлять права по иным основаниям, чем в отношении цифрового актива, например в данном контексте речь может идти о цифровом образе (аватаре), и т.д.

Соглашаясь в целом с подходом к соотношению цифрового объекта и цифрового актива как родового и видового понятий, целесообразно отметить определенную смелость авторов Модельного закона, которые указали на возможность обладания цифровым активом на праве собственности или другом вещном праве.

Кроме того, как понятие «цифровой объект», так и понятие «цифровой актив» в этом случае связываются с информационной системой, которая определена в указанном законе как набор данных, соответствующий правилам, установленным в законах страны, а также информационных технологий и технических устройств, платформа, которая обеспечивает обработку информации, создает и поддерживает условия в информационно-коммуникационной среде для взаимодействия участников гражданского оборота и учета их прав (абз. 5 ст. 3 Модельного закона о цифровых правах).

Представляется, что цифровой актив по своей природе действительно может существовать в рамках информационной системы, благодаря которой возможно удостоверение прав, предоставляемых соответствующим активом. Тем не менее цифровой объект как понятие более широкое может включать в себя и другие объекты, необязательно связанные с какой-либо

⁷ Модельный закон о цифровых правах, принят 14 апреля 2023 г. в г. Санкт-Петербурге Постановлением 55-12 на 55-м пленарном заседании Межпарламентской ассамблеи государств — участников СНГ https://iacis.ru/mod_file/p_file/1114

информационной системой, могущие существовать и вне ее, храниться на съемных материальных носителях.

Таким образом, определение цифрового объекта необходимо сформулировать следующим образом: нематериальный объект, обладающий характеристиками, отличающими его от других объектов, представленный в цифровой форме и принадлежащий его обладателю на законном основании. К числу характеристик, отличающих один цифровой объект от другого, можно отнести, например, уникальный набор данных, относящихся к конкретному объекту, уникальный идентификатор, присвоенный информационной системой и т.п. В дальнейшем в настоящей работе понятие «цифровой объект» будет использоваться как общее, родовое, включающее цифровые активы и другие объекты, в том числе, например, аккаунты в социальных сетях, аккаунты электронной почты.

Анализируя понятие цифрового актива по материалам зарубежных доктринальных источников, можно сделать вывод, что соответствующий термин используется в узком и широком смысле. При этом под цифровым активом в узком смысле понимаются только имеющие ценность токены (объекты), образованные с использованием технологии распределенного реестра, ярким примером которой является блокчейн (Armstrong & Samuels, 2022, р. 5). В широком смысле в понятие цифрового актива включаются также доменные имена, аккаунты электронной почты, цифровые записи и т.п. (Faroوقي et al., 2022, р. 428). Зачастую содержание категории цифрового актива определяется путем перечисления входящих, по мнению авторов, в это понятие объектов (Klasiček, 2023, р. 239).

В ситуации отсутствия какой-либо приемлемой дефиниции цифровых активов, для формирования правовой определенности в указанной сфере и установления правовой природы и правового режима этого цифрового объекта необходимо разработать определение, которое охватывало бы максимально все существующие на настоящий момент цифровые активы, а также могло бы быть использовано для правового регулирования при возникновении новых видов цифровых активов, которые сегодня еще неизвестны.

Кроме того, важно определить, может ли цифровой актив относиться к имуществу, могут ли в отношении него осуществляться имущественные права и, соответственно, возможно ли на следование цифрового актива.

Понятие «цифровой актив» на примере Принципов УНИДРУА о цифровых активах и частном праве

Достаточно детально понятие «цифровой актив» было проработано в Принципах Международного института унификации частного права о цифровых активах и частном праве (далее — Принципы УНИДРУА)⁸, а также в Принципах использования цифровых активов в качестве обеспечения, разработанных Европейским правовым институтом (далее также — Принципы Европейского правового института)⁹.

Принципы УНИДРУА разрабатывались с сентября 2020 г. и были приняты Руководящим советом УНИДРУА 12 мая 2023 г. Подход, который использовался при подготовке Принципов, может быть охарактеризован как функциональный и нейтральный с целью охватить максимальное

⁸ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 11 princ. 2(2) (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

⁹ European Law Institute, ELI Principles on the Use of Digital Assets as Security. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf

количество цифровых активов. Среди ключевых моментов, отраженных в Принципах УНИДРУА, следующие:

- детальное и максимально широкое определение понятия цифрового актива;
- концепция контроля в отношении цифрового актива, которая может рассматриваться как своего рода аналог владения в отношении материальных вещей;
- в Принципах указано, что в отношении цифровых активов могут осуществляться имущественные права, при этом Принципы не определяют, являются ли цифровые активы имуществом.

Документ, подготовленный УНИДРУА, состоит из введения и **19 принципов**, объединенных в **семь разделов**. Каждый принцип сопровождается подробными комментариями, которые позволяют составить более полное представление о концепциях и подходах, использованных при разработке этого документа.

В соответствии со вторым принципом, который посвящен определению основных понятий, использованных в документе, «цифровой актив есть электронная запись, в отношении которой может быть установлен контроль»¹⁰. При этом электронная запись означает информацию, которая хранится на электронном носителе и к которой может быть получен доступ¹¹. Под передачей цифрового актива понимается «альтерация» имущественного права в цифровом активе¹². Термин «передача» также включает приобретение имущественного права в конечном цифровом активе¹³.

Как видим, понятие цифрового актива сформулировано предельно широко. При этом оно привязано к двум другим основным категориям — «электронная запись» и «контроль».

В комментариях ко второму принципу подчеркивается, что, как следует из определения, электронная запись представляет собой информацию, которая находится на электронном носителе, причем к указанной информации может быть получен доступ. При этом понятие «электронный носитель» рассматривается в самом широком смысле. Данная категория охватывает любой тип цифровых носителей и применяемых технологий, независимо от того, основываются ли принципы записи на носитель на электронных эффектах или каких-либо других, например жесткие диски, принцип записи на которые основан на использовании магнитных полей, а также оптические диски, когда используются физические изменения в материале¹⁴. В Принципах указано условие о возможности получения доступа к информации, предполагающее, что информация должна быть представлена в доступной для восприятия форме. Таким образом, как электронные записи нельзя рассматривать такие формы документов, как бумажные письма или устная коммуникация, которые не архивируются на материальных носителях, а также информацию, которая содержится только в памяти человека¹⁵.

¹⁰ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 11 princ. 2(2) (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹¹ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 11 princ. 2(1) (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹² Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 11 princ. 2(5) (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹³ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 11 princ. 2(5)(b) (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹⁴ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 12–13 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹⁵ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 13 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

По вышеупомянутому определению ключевым признаком цифрового актива является возможность контроля над ним. Это означает, что даже если какой-либо объект является электронной записью, подпадающей под дефиницию *второго принципа*, но в отношении нее невозможен контроль, такой объект не будет цифровым активом.

В комментариях ко второму принципу приводятся примеры объектов, которые могут или не могут подпадать под определение цифрового актива. Так, цифровым активом является, например, виртуальная валюта (криптовалюта), обращающаяся с использованием технологии публичного блокчейна (например, биткойн). Хотя в публичном блокчейне ни один пользователь не контролирует базовый протокол соответствующей информационной системы, т.е. как раз ту самую последовательность блоков, в которой происходит сделка с цифровыми активами, а механизм консенсуса, заложенный в протокол соответствующей информационной системы, проверяет достоверность сделок, осуществляемых с использованием системы, т.е. хотя ни одно лицо не может контролировать работу такого протокола или механизма консенсуса, лицо, участвующее в сделке (например, продавец) обладает контролем над частным ключом, который позволяет этому лицу осуществлять контроль над самим цифровым активом в рамках протокола соответствующей информационной системы¹⁶.

Кроме того, в состав цифровых активов могут входить и цифровые валюты, выпускаемые центральным банком соответствующего государства (в России — цифровой рубль), поскольку указанная валюта полностью подпадает под определение цифрового актива, так как хранится на электронном носителе, а законодательство государства устанавливает, каким образом соответствующее лицо осуществляет контроль относительно указанной валюты¹⁷.

Важно отметить, что в соответствии с разъяснениями разработчиков Принципов в случаях, «когда в цифровом активе содержится информация, представляющая собой имеющую отдельную ценность совокупность данных или базу данных (например, набор сведений, данных, алгоритмов, на основе которого работает система искусственного интеллекта), а также какое-либо изображение или текстовое сообщение, в отношении такой информации применяется законодательство, регулирующее отношения по поводу интеллектуальных прав, при этом информация, существующая за пределами цифрового актива, не является его частью»¹⁸.

Необходимо обратить внимание и на то, что разработчики Принципов не включают в состав цифровых активов страницы в социальных сетях, даже если они защищены паролем. При этом авторы Принципов указывают, что отношения между пользователем и социальной сетью строятся на основании пользовательского соглашения, т.е. своего рода договора, который, как правило, запрещает приобретать пользователю какие-либо права, в том числе «право собственности» на «страницу», а также на какой-либо материал, содержащийся и размещенный пользователем в социальной сети, что не согласуется с определением контроля, сформулированным в **шестом**

¹⁶ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 15–16 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹⁷ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 16 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

¹⁸ Российской Федерации это определяется Гражданским кодексом Российской Федерации, Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», в том числе главой 4.2 указанного Закона, и положением Банка России от 3 августа 2023 г. № 820-П «О платформе цифрового рубля».

¹⁸ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 16–17 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

принципе¹⁹. Именно поэтому, по мнению авторов Принципов, страница в социальных сетях не является цифровым активом.

Следует отметить, что вопрос о правовой природе такого цифрового объекта, как страница в социальных сетях, является весьма дискуссионным.

Как было показано выше, ключевым в определении цифрового актива является понятие контроля, которое сформулировано в **шестом принципе**. Формулировки определения контроля довольно сложны и отражают специфику цифрового актива, заключающуюся прежде всего в том, что цифровой актив нематериален. Как отмечают разработчики Принципов, понятие «контроль», которое вводится в Принципах, является своего рода особым функциональным эквивалентом категории «владение», которая применима к материальному имуществу²⁰. При этом контроль над цифровым активом является вопросом факта, а не юридической концепцией.

Понятие контроля, установленное шестым принципом, выполняет как минимум две основные функции. Во-первых, оно является определяющим признаком цифрового актива, так как в соответствии со **вторым принципом** цифровым активом выступает только такая электронная запись, в отношении которой возможно установление контроля. Во-вторых, понятие контроля является основой для установления лица, которое в действительности осуществляет определенные полномочия в отношении цифрового актива, т.е. по аналогии с полномочиями, относящимися к праву собственности, осуществляет владение соответствующим цифровым активом и вправе им распоряжаться.

Необходимо отметить, что смену контроля одного лица на контроль другого следует отличать от передачи цифрового актива или доли в нем, т.е. от передачи имущественных прав. Невзирая на связь трансфера прав на цифровой актив со сменой контроля, есть ситуации, когда такая смена не возникает. Национальным законодательством может быть установлено, что при наличии некоторых обстоятельств, предусмотренных этим законодательством, «право собственности» на цифровой актив может перейти к другому лицу, причем контроль может осуществляться лицом, передавшим указанный актив. Иная ситуация также возможна, например, когда на основе норм права, применимых к указанным отношениям, переданный контроль не приводит к передаче прав, в том числе имущественных прав на цифровой актив²¹.

Принцип 6(1)(a) предусматривает наличие исключительных полномочий как неотъемлемого признака имущественных прав. Однако, как отмечают разработчики Принципов, может иметь место ситуация, при которой лицо (за исключением лица, которое на законных основаниях вправе осуществлять контроль над цифровым активом), не обладающее какими-либо правами, в том числе имущественными в отношении цифрового актива, приобретает такие полномочия без согласия и вопреки воле лица, которое обладает основанным на законе правом контроля. Такое возможно, например, когда соответствующее лицо получает закрытые ключи, необходимые для доступа к цифровому активу, с использованием взлома, кражи устройства или цифрового кошелька, на котором хранятся соответствующие ключи. Это также указывает

¹⁹ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 51–52 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²⁰ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 52 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²¹ Например, полечитель, как правило, получает контроль над цифровым активом в интересах третьего лица, но при этом не приобретает имущественных прав на этот цифровой актив. См.: Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 53 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

на сущностное различие между передачей контроля над цифровым активом и передачей прав собственности на него²².

В отношении исключительности полномочий, что предусматривается **шестым принципом**, необходимо отметить, что возможность такой исключительности обеспечивается функционированием информационной системы, в которой существует соответствующий цифровой актив или с помощью которой цифровой актив создан, причем такая система должна надежно обеспечивать как наличие таких полномочий, так и их исключительность. При этом ввиду формулировок второго и шестого принципов определяющей является именно возможность контроля лица над соответствующим цифровым активом: в случае если лицо, законно контролирующее цифровой актив, утратило такой контроль в результате противоправных действий третьих лиц, например в случае кражи электронных ключей или в других подобных случаях, такое лицо не перестает быть лицом, контролирующим цифровой актив, и имеет возможность осуществлять имущественные права в отношении такого актива по аналогии с незаконным выбытием из владения собственника материального имущества.

Что касается п. 3 **шестого принципа**, который предусматривает ослабление исключительности полномочий в рамках контроля, которая установлена в п. 1, то «принцип п. 3(а) отражает ситуацию, когда исключительность полномочий ограничивается в силу соответствующих характеристик информационной системы, в которой расположен цифровой актив, и в силу указанных характеристик контроль над цифровым активом может быть изменен в соответствии с алгоритмами такой информационной системы. Пункт 3(б) того же принципа связан с добровольными действиями лица, осуществляющего контроль над цифровым активом, например, в случае, если лицо, осуществляющее контроль, желает передать часть полномочий другим лицам в целях удобства, безопасности или в каких-либо иных целях. Например, такая ситуация может возникнуть в случае заключения соглашений, т.е. когда лицо, контролирующее цифровой актив, передает часть полномочий другому лицу. Другим примером являются ситуации с многосторонними вычислениями (multi-party computation), при которых закрытый ключ, позволяющий получать доступ к цифровому активу, разделяется на несколько фрагментов, каждый из которых необходим для выполнения транзакции»²³.

Кроме того, очень важным является п. 1 **третьего принципа**, в соответствии с которым цифровой актив может быть объектом имущественных прав. Разработчики Принципов подчеркивают, что термину «имущественные права» придается максимально широкое значение²⁴.

Понятие «имущественные права» отражает функциональный подход, согласно которому необходимо обеспечить, чтобы Принципы были применимы в большинстве юрисдикций. Имущественные права, по смыслу Принципов, подразумевают, что «права или интересы, которые физические лица могут иметь в цифровых активах, при определенных обстоятельствах могут быть противопоставлены третьим лицам²⁵, т.е. также лицам, которые необязательно являются

²² Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 53 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²³ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 56 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²⁴ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 23-25 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²⁵ Digital Assets and Private Law Working Group. (2022, March 7-9). Master Copy of the Principle and Comments (Fifth session's WG materials). Int'l Institute for the Unification of Private Law. <https://www.unidroit.org/wp-content/uploads/2022/03/W.G.5-Doc-3-Master-Copy-Principles-plus-Comments-with-Questions.pdf>

сторонами²⁶ договора»²⁷. Это также указывает на аналогичность предусмотренной Принципами правовой конструкции прав на цифровые активы праву собственности на материальные объекты, которое является абсолютным, т.е. может быть противопоставлено любым третьим лицам, а не только тем, с которыми имеются договорные отношения.

Как указано в комментариях к документу, предусмотренное **третьим принципом** положение о том, что в отношении цифровых активов могут осуществляться имущественные права, не содержит конкретную правовую концепцию или квалификацию цифровых активов. В различных юрисдикциях цифровые активы могут быть квалифицированы как собственность, товар или вещь или с применением любой другой концепции, но подобная квалификация всегда будет зависеть от конкретного применимого права и государства, применяющего или имплементирующего Принципы. При этом при имплементации необходимо установить, что цифровой актив может быть объектом имущественных прав²⁸.

Таким образом, Принципы УНИДРУА можно рассматривать как комплексный документ, носящий рекомендательный характер, который содержит максимально широкое определение цифрового актива, одним из конституирующих признаков которого является возможность установления контроля в отношении цифрового актива, что является функциональным эквивалентом владения по отношению к материальному имуществу. Кроме того, Принципами устанавливается специфический правовой режим цифрового актива, предполагающий, что в отношении цифрового актива могут осуществляться имущественные права, понимаемые в самом широком смысле, причем правоотношения по осуществлению имущественных прав в отношении цифрового актива являются абсолютными, т.е. такие имущественные права могут быть противопоставлены любым третьим лицам, а не только тем, с которыми имеются договорные отношения по поводу цифрового актива, по аналогии с правом владения вещью как одной из составляющих права собственности.

Понятие «цифровой актив» в Принципах использования цифровых активов в качестве обеспечения

Понятие цифрового актива является одним из основополагающих и в разработанном Европейским правовым институтом документе «Принципы использования цифровых активов в качестве обеспечения»²⁹, причем трактовка этого понятия несколько отличается от подходов, использованных в Принципах УНИДРУА.

Указанные Принципы являются частью большого проекта, реализуемого Европейским правовым институтом, под названием «Доступ к цифровым активам», который направлен на подготовку разъяснений для тех, кто имеет определенные права на цифровые активы, и всех, кому всё чаще приходится сталкиваться с цифровыми активами в повседневной юридической практике, в частности судей, адвокатов, нотариусов, регистраторов и судебных исполнителей. Цель

²⁶ Digital Assets and Private Law Working Group. (2022, December 19–21). Master Copy of the Principle and Comments (Seventh session's WG materials). Int'l Institute for the Unification of Private Law. <https://www.unidroit.org/wp-content/uploads/2022/12/W.G.7-Doc.-3-Issues-Paper.pdf>

²⁷ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 25 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²⁸ Int'l Institute for the Unification of Private Law, UNIDROIT Principles on Digital Assets and Private Law 24 (2023). <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>

²⁹ ELI Principles on the Use of Digital Assets as Security. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf

проекта — помочь обеспечить согласованность и способствовать гармонизации существующих законов и правовых концепций, касающихся доступа к цифровым активам³⁰.

В Принципах приводится определение цифрового актива, которое Европейским правовым институтом будет использоваться для всего проекта в целом. Применительно к цифровым активам сформулированы следующие основные дефиниции:

- «“контроль” в отношении цифрового актива означает право или фактическую способность субъекта иметь дело с такими активами и (или) аннулировать их в зависимости от обстоятельств;
- “цифровой актив” означает любую запись или иной объект, который отвечает следующим критериям:
 - (i) она хранится, отображается и управляется исключительно в электронном виде, на виртуальной платформе или через виртуальную платформу или базу данных, включая случаи, когда она представляет собой запись или образ реального, торгуемого актива, а также когда цифровой актив размещается на соответствующей платформе непосредственно или через счет посредника;
 - (ii) на нее может распространяться право контроля, владения или пользования, независимо от того, квалифицируются ли такие права по закону как имущественные, обязательственные или носящие иной характер, и
 - (iii) она может быть передана от одной стороны к другой, в том числе путем добровольного отчуждения.

Для целей данного определения не имеют значения конструктивные и эксплуатационные характеристики соответствующей платформы или базы данных, то, каким образом осуществляется защита цифрового актива от неправомерного копирования, или представляет ли соответствующий цифровой актив денежное требование (и, соответственно, обязательство) идентифицируемой стороны в качестве его эмитента, хранителя или контролера, или выполняет ли рассматриваемый актив функции денег или валюты».

Как видим, и в этом определении понятие «контроль» является конституирующим признаком цифрового актива.

Необходимо отметить некоторое отличие концепции контроля, которая используется в Принципах Европейского правового института, от категории контроля, отраженной в Принципах УНИДРУА. В Принципах Европейского правового института используется гибридная концепция контроля над цифровым активом, которая охватывает как юридическое «владение» конкретным лицом (примером является осуществление этим лицом законного права контролировать этот цифровой актив в случаях, когда последний признается объектом права собственности в конкретной юрисдикции или пользуется иным, аналогично защищенным правовым режимом), так и простой, фактический контроль лица над цифровым активом (например, любая форма контроля, за исключением владения в легальном смысле, когда цифровой актив в конкретной юрисдикции не является объектом права собственности на основании соответствующих правовых норм)³¹. Легальный (юридический) или фактический контроль будет (в определенных случаях — может быть) достаточным для того, чтобы имущественный интерес

³⁰ Подробную информацию о проекте см. на сайте института: <https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/eli-enforcement-against-digital-assets/>

³¹ Digital Assets and Private Law Working Group. (2022, March 7–9). Master Copy of the Principle and Comments (Fifth session's WG materials). Int'l Institute for the Unification of Private Law. <https://www.unidroit.org/wp-content/uploads/2022/03/W.G.5-Doc.-3-Master-Copy-Principles-plus-Comments-with-Questions.pdf>

в отношении цифрового актива был сформирован, но определяющей формой контроля, которая имеет отношение к созданию имущественного интереса в указанном активе, является фактический контроль³². Кроме того, что фактический контроль является надлежащей формой контроля для формирования имущественного интереса применительно к цифровым активам, он также необходим для тех цифровых активов, в которых имущественные права в строгом смысле могут не существовать с учетом их особенностей, которые, согласно внутригосударственному праву, исключают их отнесение к объектам права собственности.

Гибридная концепция контроля, которая используется в Принципах Европейского правового института, не предполагает, что для формирования цифрового актива необходимо наличие как юридического, так и фактического контроля. Любого из видов контроля достаточно для формирования имущественного интереса в цифровом активе. При этом только фактический контроль необходим для формирования имущественного интереса в цифровом активе.

Согласно позиции авторов комментариев к Принципам Европейского правового института, определение, предложенное в Принципах, сфера действия которых охватывает как криптоактивы, так и цифровые активы, не прошедшие криптографическую аутентификацию, и которые применяются к ним одинаковым образом, опирается на следующие три основных атрибута цифровых активов: во-первых, нематериальный характер, который проявляется в их хранении, отображении и (или) администрировании только в электронном виде, даже если конкретный актив отражает или привязан к материальному, реальному активу; во-вторых, право контроля, владения или пользования, в широком смысле определяемое как право на доступ и пользование нетрадиционной формой стоимости, которую воплощает цифровой актив, — это право в сочетании с их цифровым форматом делает их передачу и последующее использование коммерчески привлекательными; в-третьих, возможность передачи. Указанный третий атрибут можно также определить как оборотоспособность цифрового актива.

Таким образом, Принципы Европейского правового института можно рассматривать как документ, носящий рекомендательный характер, в котором представлено понятие цифрового актива. Его основным признаком является возможность юридического и фактического контроля над указанным активом, который обладает таким свойством, как передаваемость (transferability), или оборачиваемость.

Заключение

Понятия «цифровой объект» и «цифровой актив» приобретают всё большую актуальность в связи с цифровизацией. К определению объема и содержания указанных категорий, а также их соотношения имеются различные подходы как в доктринальных, так и в нормативных источниках. В некоторых случаях предпринимаются попытки сформулировать максимально широкие определения данных понятий; в некоторых случаях цифровые активы трактуются в узком смысле и включают в себя лишь определенное число цифровых объектов. Иногда высказывается мнение, что к цифровым объектам и активам может быть применен режим права собственности или вещных прав. Некоторые ученые рассматривают указанные объекты как объекты особого рода, требующие отдельного правового регулирования.

³² Digital Assets and Private Law Working Group. (2022, March 7–9). Master Copy of the Principle and Comments (Fifth session's WG materials). Int'l Institute for the Unification of Private Law. <https://www.unidroit.org/wp-content/uploads/2022/03/W.G.5-Doc-3-Master-Copy-Principles-plus-Comments-with-Questions.pdf>

По итогам проведенного исследования понятие цифрового объекта можно сформулировать следующим образом: цифровой объект — нематериальный объект, обладающий характеристиками, отличающими его от других объектов, представленный в цифровой форме и принадлежащий его обладателю на законном основании. Цифровой объект можно рассматривать как общее, родовое понятие, включающее в себя в том числе цифровые активы и другие объекты, например, аккаунты в социальных сетях, аккаунты электронной почты.

Анализируя термин «цифровой актив», можно сделать вывод, что он может пониматься в широком и в узком смысле, как было показано в настоящем исследовании. При этом для формирования правовой определенности в указанной сфере и выяснения правовой природы и правового режима цифрового актива необходимо разработать определение, которое охватывало бы все существующие на настоящий момент цифровые активы, а также могло бы быть использовано для правового регулирования при возникновении новых видов цифровых активов, которые сегодня еще неизвестны. Значимые попытки сформулировать понятие цифрового актива были предприняты в рамках УНИДРУА и Европейского правового института, причем существенным, конституирующим признаком цифрового актива стало понятие контроля в отношении цифрового актива.

Четкое и понятное разграничение понятий «цифровой объект» и «цифровой актив» будет способствовать формированию надлежащего правового регулирования в указанной сфере и обеспечению защиты прав субъектов, вовлеченных в соответствующие правоотношения. Разграничение указанных двух понятий необходимо потому, что суть и правовая природа цифровых активов, их оборот требуют особого правового регулирования с учетом специфики цифровых активов, а также потому, что цифровые объекты можно включать в перечень объектов гражданских прав в тех правопорядках, где теория объектности имеет значение.

Список литературы / References

1. Armstrong, D., & Samuels, M. (2022). *Bloomsbury professional law insight—Cryptocurrency in matrimonial finance*. Bloomsbury Publishing Plc.
2. Ayusheeva, I. Z. (2021). Tsifrovyye ob"yekty grazhdanskikh prav [Digital objects of civil rights]. *Lex russica*, 74(7), 32–43. <https://doi.org/10.17803/1729-5920.2021.176.7.032-043>
3. Brennen, S. J., & Kreiss, D. (2016). Digitalization. In K. B. Jensen, R. T. Craig, J. D. Pooley, & E. W. Rothenbuhler (Eds.) *The international encyclopedia of communication theory and philosophy* (pp. 1–11). John Wiley & Sons. <https://doi.org/10.1002/9781118766804.wbiect111>
4. Fairfield, J. (2023). Property as the law of virtual things ["Veshchnoye" pravo virtual'nykh "veshchey"] (A.M. Doiev, trans.). *Digital Law Journal*, 4(3), 16–39. <https://doi.org/10.38044/2686-9136-2023-4-3-16-39>
5. Farooqui, M. O., Sharma, B., & Gupta, D. (2022). Inheritance of digital assets: Analyzing the concept of digital inheritance on social media platforms. *Novum Jus*, 16(3), 413–435. <https://doi.org/10.14718/NovumJus.2022.16.3.15>
6. Faulkner, P., & Runde, J. (2019). Theorizing the digital object. *Management Information Systems Quarterly*, 43(4), 1279–1302. <https://misq.umn.edu/theorizing-the-digital-object.html>
7. Hagberg, J., Sundstrom, M., & Egels-Zandén, N. (2016). The digitalization of retailing: An exploratory framework. *International Journal of Retail and Distribution Management*, 44(7), 694–712.
8. Hui, Y. (2012). What is a digital object? *Metaphilosophy*, 43(4), 380–395. <https://doi.org/10.1111/j.1467-9973.2012.01761.x>

9. Ivanov, A. A. (2023). Tsifrovizatsiya i veshchnyye prava. Fragment iz tsikla lektsiy “Grazhdanskoye pravo i tsifrovizatsiya”. [Digitalization and ius ad rem. An excerpt from the lecture series “Civil Law and Digitalization”]. *Zakon*, (7), 43–52.
10. Kallinikos, J., Aaltonen, A. V., & Marton, A. (2010). A theory of digital objects. *First Monday*, 15(6). <https://doi.org/10.5210/fm.v15i6.3033>
11. Klasiček, D. (2023). Inheritance law in the twenty-first century: New circumstances and challenges. In O. J. Gstrein, M. Fröhlich, C. van den Berg, & T. Giegerich (Eds.), *Modernising European Legal Education (MELE)* (pp. 235–251). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-40801-4_15
12. Koles, B., & Nagy, P. (2021). Digital object attachment. *Current Opinion in Psychology*, 39, 60–65. <https://doi.org/10.1016/j.copsyc.2020.07.017>
13. Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, 63, Article 102466. <https://doi.org/10.1016/j.ijinfomgt.2021.102466>
14. Lyons, P. A. (1998). Managing access to digital information: Some basic terminology issues. *Bulletin of the American Society for Information Science and Technology*, 24(2), 21–24. <https://doi.org/10.1002/bult.81>
15. Melnikova, T. V., Nikitashina, N. A., & Schalyaeva, J. V. (2023). Tsifrovyye finansovyye aktivy kak ob"yekty grazhdanskikh prav [Digital financial assets as objects of civil rights]. *Jurist [The Lawyer]*, (11), 37–42.
16. Sklovskiy, K. I. (2023). *Sobstvennost' v grazhdanskom prave [Property in civil law]* (6th ed.). Statut.
17. Srai, J. S., & Lorentz, H. (2019). Developing design principles for the digitalisation of purchasing and supply management. *Journal of Purchasing and Supply Management*, 25(1), 78–98. <https://doi.org/10.1016/j.pur-sup.2018.07.001>
18. Sukhanov, E. A. (2021). O grazhdansko-pravovoi prirode “tsifrovogo imushchestva” [On the civil legal nature of “digital property”]. *Vestnik grazhdanskogo prava [Civil Law Review]*, 21(6), 7–29.
19. Velichko, V. E., & Evstigneve, E. A. (2019). Tsifrovyye prava v Rossii: dvizheniye vpered ili beg po krugu? [Digital rights in Russia: Moving forward or running in circles?]. *Zhurnal Zhurnal rossiyskoy shkoly chastnogo prava [Journal of the Russian Private Law School]*, (2), 48–59.
20. Volos, A. (2022). Digitalization of society and objects of hereditary succession. *Law Journal of the Higher School of Economics*, 15(3), 51–71. <https://doi.org/10.17323/2072-8166.2022.3.51.71>

Сведения об авторе:

Шипикова А. Г. — соискатель, кафедра интеграционного права и прав человека, МГИМО МИД России, судья Московского городского суда, Москва, Россия.

shipikova@mail.ru

Information about the author:

Anna G. Shipikova — Ph.D. Scholar, Department of Integration Law and Human Rights, MGIMO-University, Judge of the Moscow City Court, Moscow, Russia.

shipikova@mail.ru

РЕЦЕНЗИЯ НА КНИГУ

РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОЕКТ НИДЕРЛАНДОВ

Ю. В. Волков

Уральский государственный юридический университет
имени В. Ф. Яковлева
620066, Россия, Екатеринбург, ул. Комсомольская, 21

Рецензия на книгу

Sheikh, H., Prins, C., & Schrijvers, E. (2023). *Mission AI: The new system technology*. Springer. <https://doi.org/10.1007/978-3-031-21448-6>

Ключевые слова

алгоритм, данные, право, искусственный интеллект, регулирование, система

Для цитирования

Волков, Ю. В. (2024). Регулирование искусственного интеллекта: проект Нидерландов. *Цифровое право*, 5(2), 69–75. <https://doi.org/10.38044/2686-9136-2024-5-2-2>

Поступила: 12.04.2024, принята в печать: 19.05.2024, опубликовано: 28.06.2024

BOOK REVIEW

REGULATING ARTIFICIAL INTELLIGENCE: THE NETHERLANDS PROJECT

Yuriy V. Volkov

Ural State Law University
21 Komsomolskaya St., Ekaterinburg, Russia, 620137

Review of a book

Sheikh, H., Prins, C., & Schrijvers, E. (2023). *Mission AI: The new system technology*. Springer. <https://doi.org/10.1007/978-3-031-21448-6>

Keywords

algorithm, data, law, artificial intelligence, regulation, system

For citation

Volkov, Y. V. (2024). Regulating artificial intelligence: The Netherlands project. *Digital Law Journal*, 5(2), 69–75. <https://doi.org/10.38044/2686-9136-2024-5-2-2>

Submitted: 12 Apr. 2024, accepted: 19 May 2024, published: 28 June 2024

Различных изданий, основной темой которых является искусственный интеллект (ИИ), выпущено за прошедшие два-три года значительное число. Российские системы научной индексации позволяют идентифицировать более 157 тыс. Если ограничить поиск словосочетанием «ИИ и право», то результат будет также весьма внушительным — более 9000 статей. Однако в российском обороте (в перечне цитат и в библиотечных фондах) не так много современных зарубежных научных изданий. В этой связи, полагаем, будет актуальным представить еще одно. Книга *“Mission AI: The new system technology”* («Миссия ИИ: Новая системная технология» представляет собой научную адаптацию и перевод на английский язык отчета Голландского научного совета по государственной политике под наименованием *“Opgave AI. De Nieuwe Systeemtechnologie”* («Задача ИИ. Новые системные технологии»)¹. Документ был представлен голландскому правительству в 2021 г. В исследовании искусственный интеллект определяется как «системная технология», которая коренным образом меняет общество и устанавливает пять всеобъемлющих задач по внедрению ИИ.

Авторский (редакторский) состав: профессор Кориен Принс (*Corien Prins* — основатель и с 1995 г. руководитель Тилбургского института права, технологий и общества, с 2017 г. она назначена председателем Нидерландского научного совета по государственной политике); Харун Шейх (*Haroon Sheikh* — старший научный сотрудник и координатор проектов в Голландском научном совете по государственной политике и профессор по стратегическому управлению глобальными технологиями в Амстердамском свободном университете (*VU*)); Эрик Шрайверс (*Erik Schrijvers* — доктор Утрехтского университета, в 2016–2017 гг. исследователь группы «Информационное общество и правительство» Министерства внутренних дел Нидерландов). Редакторы изучили академическую литературу, политические документы, провели интервью со 175 экспертами из разных стран (не только из Нидерландов). Книга включают также интервью с муниципальными и государственными служащими, представителями компаний, деятелями гражданского общества и членами Голландской коалиции ИИ. На заключительном этапе материалы рассмотрели и дали ценные предложения профессор, доктор Люк Стилс (*Luc Steels* — почетный профессор искусственного интеллекта, Свободный университет Брюсселя²), Марлен Стиккер и Том Демейер (*Tom Demeyer* — директор и технический директор *Waag*), профессор, доктор Ставрос Зуридис (*Stavros Zouridis* — член Совета по безопасности Нидерландов,

¹ Более подробная информация о докладе доступна по адресу: <https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie> См. краткое содержание доклада на английском языке: Prins, C., Sheikh, H., Schrijvers, E., de Jong, E., Steijns, M., & Bovens, M. (2021). *Mission AI: The new system technology*. Netherlands Scientific Council for Government Policy. https://www.wrr.nl/binaries/wrr/documenten/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie/Summary-WRRreport_Mission+AI_The+New+System+Technology_R105.pdf

² См., в частности, одну из влиятельных работ профессора Стилса в области искусственного интеллекта в соавторстве с Р. де Мантэрас — Барселонскую декларацию о надлежащем развитии и использовании искусственного интеллекта (Steels & Mantaras, 2018).

LL.M)³, профессор, доктор Хосе ван Дейк (*Jose van Dijck* — профессор медиаисследований, Утрехтский университет)⁴, профессор, доктор Коэн Френкен (*Koen Frenken* — профессор инновационных исследований, Утрехтский университет)⁵.

Издание состоит из введения, которое позиционировано как первая глава, и трех частей. В первой части (из трех глав) исследованы социальная интеграция ИИ, определение ИИ и его интерпретации как системной технологии. Глава 2 анализирует, что такое ИИ, как можно определить технологию и какой выбор необходимо сделать. После этого описано историческое развитие знаний об искусственном интеллекте с 1950 г. Глава 3 посвящена разработкам последних лет: ИИ в науке; практический потенциал ИИ; искусственный интеллект в сферах инвестирования, экономики и занятости. В частности, в п. 3.1.5 рассмотрен характерный для США, Европы и Британии вопрос фокусировки государственного управления на проблемах, связанных с ИИ. Особенно иллюстративен график (Sheikh et al., 48), на котором зафиксирован экспоненциальный рост количества направлений, связанных с ИИ, в 2015–2020 гг.: научных статей; заявок на патенты; инвестиционных проектов; национальных стратегий. В главе 4 дается разъяснение, какой тип технологии представляет собой ИИ, обобщены и классифицированы ИИ-технологии. Отдельно рассмотрен генеративный языковой трансформер (*Generative Pre-trained Transformer, GPT*) как система ИИ. Отдельно показан ИИ как система различных технологий. Проведено сравнение ранних и более поздних моделей ИИ. Освещен вопрос технико-экономической парадигмы ИИ. Подразделы 4.3–4.7 отведены под постановку пяти задач: демистификации; контекстуализации; участия гражданского общества; регулирования; позиционирования (Sheikh et al., 85–130).

Часть II составляет ядро анализа. В главах 5–9 рассмотрены по очереди пять задач социальной интеграции ИИ, которые были кратко обозначены в первой части: **демистификация (demystification), контекстуализация (contextualization), вовлечение (engagement), регулирование (regulation) и позиционирование (international positioning)**.

Демистификация (demystification) относится к пониманию обществом ИИ, как технологии, и зависит от осознанного восприятия того, на что способен ИИ и на что нет сейчас и в будущем. Какие существуют мифы о том, как работает ИИ, о его вероятном будущем влиянии и о цифровых технологиях в целом. В частности, авторы отмечают, что «голландцы весьма обеспокоены потерей рабочих мест и устранением “человеческого фактора”» (Sheikh et al., 139).

Контекстуализация (contextualization) — это применение системы ИИ в определенном контексте, в определенном окружении, от которого зависит то, как она будет работать. Первый аспект, отмеченный авторами, — формирование и принятие обществом «технологических экосистем». Быстро развивающаяся технология ИИ эволюционирует параллельно с «поддерживающими технологиями» (Sheikh et al., 182). К их числу авторы относят такие технологии, как сети нового поколения 5G, которые представляют собой скачок вперед с точки зрения скорости, а также технологию «интернет вещей» (*IoT*). Это вызов для всех участников,

³ Профессор С. Зуридис, специализирующийся на конституционном и административном праве, ведет исследовательскую работу в области приложения искусственного интеллекта к принятию решений государственными органами. См., к примеру, подготовленную в соавторстве влиятельную работу по влиянию ИИ на дискрецию должностных лиц (Zouridis et al., 2019).

⁴ Профессор Хосе ван Дейк — автор множества публикаций по вопросу регулирования цифровых платформ: приведем лишь некоторые наиболее цитируемые работы: van Dijck (2020), van Dijck (2021), van Dijck et al. (2023).

⁵ Профессор К. Френкен — участник следующих значимых исследований цифровой экономики: Punt et al. (2023), van Slageren et al. (2023), Koutsimpogiorgos et al. (2023); Wanzenböck et al. (2020).

вовлеченных в развертывание и реализацию ИИ, его функциональности в определенных областях. Интеграция систем ИИ, например, систем массового наблюдения, и растущая зависимость от частных поставщиков этих систем и цифровых услуг.

Вовлечение (engagement) относится к социальной обстановке вокруг систем ИИ, в частности внедрению социальных экосистем. Если не будет достаточного вовлечения систем ИИ, то на карту, по мнению авторов, будут поставлены такие основные права, как равенство, конфиденциальность, автономия, а также демократические принципы (инклюзивность, плюрализм). Нормативная база является важной предпосылкой для формирования этого участия, что обуславливает четвертую задачу.

Регулирование (regulation) действует на уровне общества в целом, фокусируясь на вопросе, какие правила и структуры требуются. Когда новая технология покидает лабораторию, изначально трудно контролировать, адаптировать или разрабатывать необходимые структуры. Многие еще неясно о ее природе и эффектах, и поэтому, пока ИИ еще не внедрен во все сферы общества, трудно понять, какие конкретные гражданские ценности он может поставить под угрозу. На раннем этапе технологические компании часто продвигают саморегулирование сектора или утверждают, что на самих пользователей можно положиться в деле защиты определенных ценностей. Постепенно, однако, выявляются структурные проблемы, требующие более активной роли правительства. Так, авторы приводят в качестве примера сеть Facebook⁶, которая использует технологию «черный ящик», связанную с глубинным обучением ИИ. Опасность, по мнению авторов, заключается в том, что невозможно выяснить, почему какое-либо сообщение появилось или нет в чьей-то ленте новостей. Это необязательно означает, что процесс принципиально непонятен, просто задача выяснения того, как система приходит к конкретному решению, очень сложна и недоступна обычному пользователю. Дальнейшее применение такого рода технологий на основе алгоритмов ИИ возможно и при фальсификации результатов выборов и т.д. Авторы приводят и другие примеры сетей, которым присущи аналогичные недостатки. По мере того как технология глубже укореняется в обществе, она всё больше затрагивает гражданские ценности, которые подпадают под ответственность правительства. Со временем более широкие социальные эффекты новой технологии становятся яснее, и поэтому политика и законодательство конкретизируются. По этой причине необходимо разрабатывать более широкие меры государственного регулирования. Впоследствии акцент саморегулирования ИИ сместился на государственное регулирование (авторы используют фразу «активное вмешательство правительства», подражая проекту Закона Европейского союза об ИИ, который был принят уже после выхода издания). В то же время выявляются и другие структурные проблемы. Авторы подчеркивают, что не существует панацеи или «серебряных пуль» для регулирования системных технологий. Правильное внедрение технологии в общество требует широкого набора мер, разработанных в течение длительного периода времени. Примером является двигатель внутреннего сгорания, который сделал возможным появление автомобиля: ремни безопасности, страхование, номерные знаки, подушки безопасности, экзамены по вождению, правила дорожного движения и дорожные знаки были шагами, которые способствовали его социальной интеграции — процессу, который продолжается и по сей день, поскольку автомобиль и его среда

⁶ Признана экстремистской и запрещена в Российской Федерации в соответствии с федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации»)

постоянно развиваются. Было невозможно предвидеть, что все эти меры будут необходимы, когда автомобиль был впервые представлен.

Позиционирование (international positioning) — это международная задача позиционирования страны в области ИИ, которая связана с предыдущими задачами, но только на международном уровне в рамках Европейского союза. Задача позиционирования касается таких вопросов, как безопасность, научные разработки, развертывание сетей 5G, внедрение инфраструктуры данных, которые жизненно важны для общества, но по-разному принимаются и регулируются в каждой отдельно взятой стране.

В части III рассмотрены последствия анализа для политики. Глава 10 доносит основные идеи и связывает пять задач с рекомендациями: по две рекомендации для каждой задачи с конкретными пунктами действий.

Демистификация:

- Сделать изучение ИИ и его потенциальных приложений государственной функцией.
- Стимулировать «ИИ-грамотность» населения, начиная с создания регистров алгоритмов.

Контекстуализация:

- Разработать национальную идентичность ИИ, исследовать корректировки для технической экосистемы в соответствующих областях.
- Укрепить навыки и критические возможности лиц, работающих с системами ИИ, разработать структуры обучения и сертификации.

Вовлеченность:

- Укрепить потенциал организаций гражданского общества в цифровую эпоху с использованием ИИ.
- Проверить эффективные циклы обратной связи между разработчиками и пользователями ИИ.

Регулирование:

- Поставить на законодательную повестку вопросы регулирования ИИ и организации цифровой среды обитания.
- Использовать законодательство для активного управления разработками, связанными с наблюдением и сбором данных, конфликтом интересов между государственными и частными интересами в цифровой сфере.

Позиционирование:

- Укрепить конкурентоспособность Нидерландов с помощью «дипломатии ИИ» в рамках ЕС.
- Развивать знания, необходимые для обеспечения обороны Нидерландов в эпоху ИИ. Укрепить обороноспособность в «информационной войне» и защиту от экспорта «цифровой диктатуры».

Заключительная рекомендация: создать правительственную инфраструктуру для ИИ, начиная с координационного центра.

Отчет был написан для голландского правительства, и практические последствия рекомендаций специфичны для Нидерландов. Однако сами рекомендации универсальны и, по мнению авторов, могут быть актуальны и для других стран.

Издание носит несколько претенциозное наименование «Миссия ИИ». Естественно, авторы не придают ИИ статуса субъекта. Искусственный интеллект — это раздел информатики (практически все учебные издания по теме информатики включают такой или аналогичный раздел) уже более двух десятков лет. Соответственно, использовать термин «искусственный интеллект» без соответствующего контекста (система ИИ, приложение ИИ и т. д.), как это было

популярно в 1960-е гг., в настоящее время не вполне корректно. Однако значимость технологий ИИ, выход ИИ «из лабораторий» в широкую жизнь, влияние на повседневные нужды, права и обязанности современного человека позволяют утверждать, что современный мир живет в эпоху систем ИИ. Обозначенные авторами «пять задач», «пять переходов» следует рассматривать как авторское экспертное видение проблемы. Они подчеркивают, что предложенные решения касаются голландского общества. При этом именно Нидерланды являются пока единственной страной в мире — поставщиком автоматизированных литографических комплексов, которые производят заготовки для компьютерных чипов. Иными словами, голландцы первыми сталкиваются с проблематикой внедрения передовых информационных технологий, в том числе технологий ИИ, в современную жизнь. Соответственно, и новые правовые проблемы в сфере применения систем ИИ они начинают решать первыми. В качестве критического замечания можно отметить обобщенный теоретический подход авторов к проблеме.

В действительности первые шаги по контролю использования алгоритмов ИИ были сделаны уже после выхода отчета. 19 января 2021 г. парламент Нидерландов принял предложение о создании регистра алгоритмов⁷. В России от аналогичного решения пока отказались. В свою очередь в Англии 28 декабря 2024 г. на обсуждение был поставлен законопроект о контроле использования системами ИИ персональных данных (Data (Use and Access) Bill)⁸. Британское сообщество юристов рассматривает реестры алгоритмов как правовой инструмент и выступает за его внедрение в уголовное право. Европейская комиссия также планирует введение реестра алгоритмов. Другая затронутая в издании правовая проблема, которая касается повседневной жизни любой страны, — цифровая среда обитания (в России — цифровая среда доверия). Авторы только ставят данную проблему. В целом отсутствие конкретных правовых решений и постановочный, описательный формат издания можно объяснить тем, что работа выполнялась для правительственных структур. Однако, несмотря на отдельные замечания, книга представляет несомненный интерес для исследователя. Описанные в издании проблемы могут быть присущи любому обществу и каждой социальной системе. Нидерланды, обладая передовыми технологиями, столкнулись с социальными и правовыми последствиями внедрения технологий ИИ раньше других. Тем самым для многих следующих юрисдикций есть шанс реализовать «преимущество отстающего», а именно не повторять ошибки идущего первым.

Несколько слов о том, кому будет полезно данное издание. Предполагаем, что все студенты-юристы (уровня специалитета и магистратуры), планирующие профессиональную деятельность с использованием компьютерных технологий, должны как минимум обратить внимание на данную книгу, а лучше прочитать ее. Особое внимание следует уделить четвертой задаче (регулированию) во второй главе.

Кроме того, издание может быть полезно специалистам сферы информационных технологий и информационной безопасности. Многие проблемы решаются технологически на стадии разработки систем и алгоритмов, соответственно, и внедрение технических и технологических систем ИИ в жизнь может быть реализовано более успешно и быстро. Книга будет любопытна преподавателям, а также всем, кто интересуется технологиями искусственного интеллекта.

⁷ Ныне регистр доступен по адресу: <https://algoritmes.overheid.nl/en>

⁸ Data (Use and Access) Bill 2024-25, HL Bill (UK).

Список литературы / References

1. Koutsimpogiorgos, N., Frenken, K., & Herrmann, A. M. (2023). Platform adaptation to regulation: The case of domestic cleaning in Europe. *Journal of Industrial Relations*, 65(2), 156–184. <https://doi.org/10.1177/00221856221146833>
2. Punt, M. B., van Kollem, J., Hoekman, J., & Frenken, K. (2023). Your Uber is arriving now: An analysis of platform location decisions through an institutional lens. *Strategic Organization*, 21(3), 501–536. <https://doi.org/10.1177/14761270211022254>
3. Sheikh, H., Prins, C., & Schrijvers, E. (2023). *Mission AI: The new system technology*. Springer. <https://doi.org/10.1007/978-3-031-21448-6>
4. Steels, L., & De Mantaras, R. L. (2018). The Barcelona declaration for the proper development and usage of artificial intelligence in Europe. *AI Communications*, 31(6), 485–494. <https://doi.org/10.3233/AIC-180607>
5. van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law and Security Review*, 36. Article 105377. <https://doi.org/10.1016/j.clsr.2019.105377>
6. van Dijck, J. (2021). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media and Society*, 23(9), 2801–2819. <https://doi.org/10.1177/1461444820940293>
7. van Dijck, J., de Winkel, T., & Schäfer, M. T. (2023). Deplatformization and the governance of the platform ecosystem. *New Media and Society*, 25(12), 3438–3454. <https://doi.org/10.1177/14614448211045662>
8. van Slageren, J., Herrmann, A. M., & Frenken, K. (2023). Is the online gig economy beyond national reach? A European analysis. *Socio-Economic Review*, 21(3), 1795–1821. <https://doi.org/10.1093/ser/mwac038>
9. Wanzenböck, I., Wesseling, J. H., Frenken, K., Hekkert, M. P., & Weber, K. M. (2020). A framework for mission-oriented innovation policy: Alternative pathways through the problem-solution space. *Science and Public Policy*, 47(4), 474–489. <https://doi.org/10.1093/scipol/scaa027>
10. Zouridis, S., van Eck, M., & Bovens, M. (2019). Automated discretion. In T. Evans & P. Hupe (Eds.), *Discretion and the Quest for Controlled Freedom* (pp. 313–329). https://doi.org/10.1007/978-3-030-19566-3_20

Сведения об авторе:

Волков Ю. В. — кандидат юридических наук, доцент, доцент кафедры информационного права, Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия.

yurii.volkov@usla.ru

ORCID: <https://orcid.org/0000-0001-9917-717X>

Information about the author:

Yuriy V. Volkov — Ph.D. in Law, Associate Professor, Associate Professor of the Information Law Department, Ural State Law University, Ekaterinburg, Russia.

yurii.volkov@usla.ru

ORCID: <https://orcid.org/0000-0001-9917-717X>

